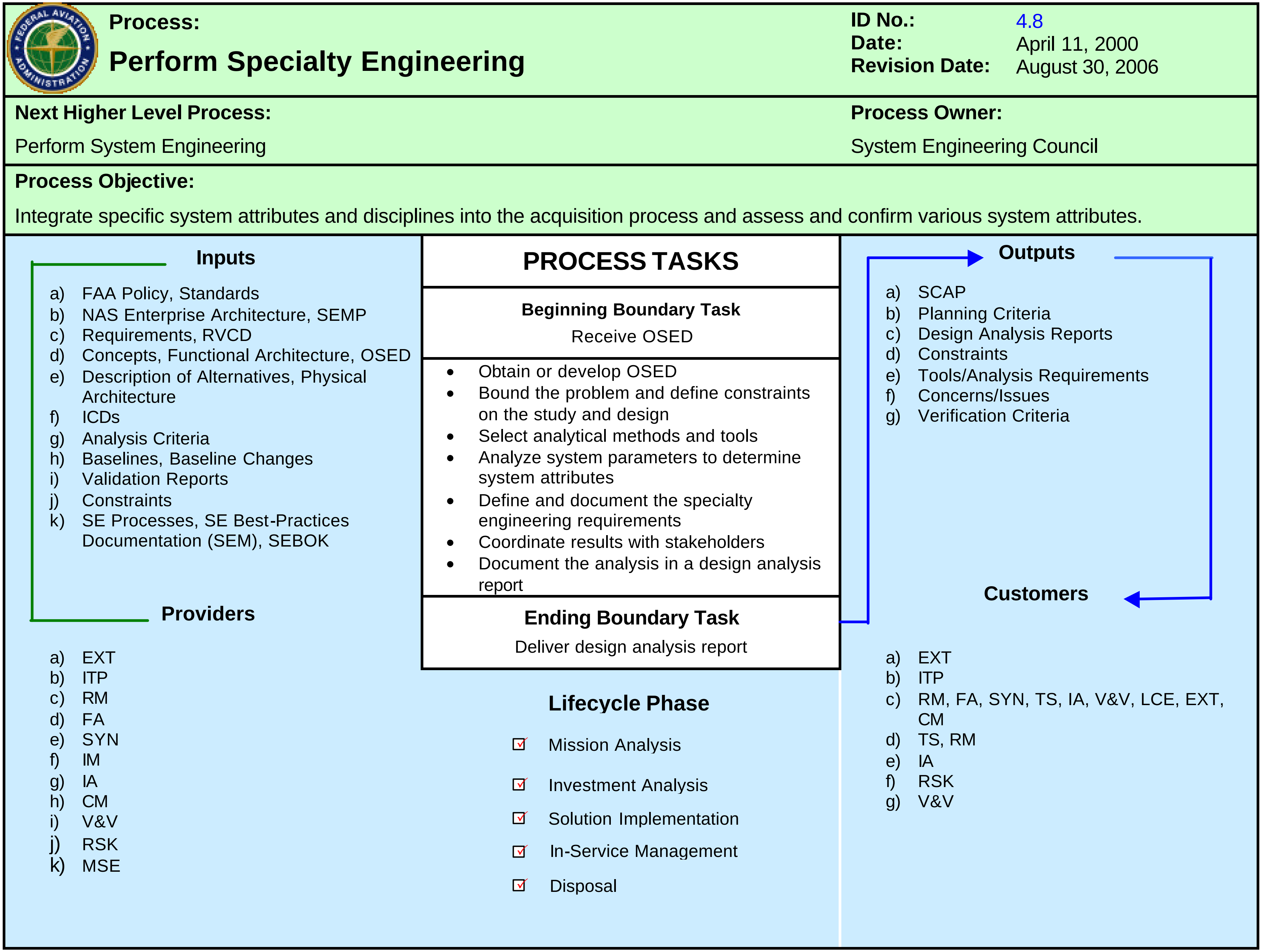
4.8 Specialty Engineering

Specialty Engineering is a subset of System Engineering (SE) that defines and evaluates specific areas, features, and/or characteristics of a system. Specialty Engineering supplements the acquisition process by defining these characteristics and assessing their impact on the program. SE relies on specialty domain expertise to define and characterize specific requirements. SE's function in this process is to integrate the design engineer's activities and specialty engineer's activities, coordinate and open communication lines between the design engineer and specialty engineer, and focus the engineering effort on meeting the common goal of satisfying the customer—not on performing detailed Specialty Engineering work.

Engineers with specialized engineering skills conduct Specialty Engineering by primarily performing system analyses. These skill areas include System Safety Engineering (SSE); Reliability, Maintainability, and Availability (RMA); Human Factors Engineering; Electromagnetic Environmental Effects (E^3); Quality Engineering; Information Security Engineering; and Hazardous Materials Management/Environmental Engineering. Engineers in these disciplines perform analyses throughout the system's lifecycle. The results are used to derive, validate, and verify requirements; evaluate system design progress and technical soundness; and manage risk. At a minimum, reports on the analysis results are available at standard design milestones, including the design, acquisition, and program reviews. When a supplier is involved, deliverables comply with contract requirements. Figure 4.8-1 shows the general process for performing Specialty Engineering, listing the key inputs to initiate the task, providers, process tasks, outputs required, and customers of process outputs.



Process:

Perform Specialty Engineering

ID No.: 4.8
Date: April 11, 2000
Revision Date: August 30, 2006

Next Higher Level Process:

Perform System Engineering

Process Owner:

System Engineering Council

Process Objective:

Integrate specific system attributes and disciplines into the acquisition process and assess and confirm various system attributes.

Inputs

a) FAA Policy, Standards
b) NAS Enterprise Architecture, SEMP
c) Requirements, RVCD
d) Concepts, Functional Architecture, OSED
e) Description of Alternatives, Physical Architecture
f) ICDs
g) Analysis Criteria
h) Baselines, Baseline Changes
i) Validation Reports
j) Constraints
k) SE Processes, SE Best-Practices Documentation (SEM), SEBOK

Providers

a) EXT
b) ITP
c) RM
d) FA
e) SYN
f) IM
g) IA
h) CM
i) V&V
j) RSK
k) MSE

PROCESS TASKS

Beginning Boundary Task

Receive OSED

- Obtain or develop OSED
- Bound the problem and define constraints on the study and design
- Select analytical methods and tools
- Analyze system parameters to determine system attributes
- Define and document the specialty engineering requirements
- Coordinate results with stakeholders
- Document the analysis in a design analysis report

Ending Boundary Task

Deliver design analysis report

Lifecycle Phase

☑ Mission Analysis

☑ Investment Analysis

☑ Solution Implementation

☑ In-Service Management

☑ Disposal

Outputs

a) SCAP
b) Planning Criteria
c) Design Analysis Reports
d) Constraints
e) Tools/Analysis Requirements
f) Concerns/Issues
g) Verification Criteria

Customers

a) EXT
b) ITP
c) RM, FA, SYN, TS, IA, V&V, LCE, EXT, CM
d) TS, RM
e) IA
f) RSK
g) V&V

Figure 4.8-1. Specialty Engineering Process-Based Management Chart

4.8.0 Introductory Material

4.8.0.1 Introduction to Specialty Engineering

Engineers conduct Specialty Engineering throughout the system's lifecycle. Specialty Engineering analyses are conducted early to derive and validate requirements. In addition, the Specialty Engineering disciplines support the Functional Analysis (Section 4.4), Synthesis (Section 4.5), and Trade Studies (Section 4.6) efforts in selecting and designing solutions to requirements. Later in the lifecycle, after requirements at all levels are validated, these analyses provide support in verifying requirements by describing and assessing the characteristics of the design and/or operations. As early as possible in the lifecycle, the Specialty Engineering disciplines find and resolve potential program risk. Finding and controlling risk early assists decision makers in seeking the lowest possible cost and increases the probability of program success and operator acceptance of the product.

This section describes the functions, objectives, and products of the various Specialty Engineering disciplines.

4.8.0.1.1 Description of Specialty Engineering Disciplines

Specialty Engineering analyses present characteristics of the system from a specific technical perspective. Table 4.8-1 gives a general description of the Specialty Engineering disciplines.

Table 4.8-1. Specialty Engineering Disciplines

Specialty Engineering Discipline	Description
SSE	Evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, and safety risk assessments and in hazard tracking and control.
RMA	Quantitative and qualitative analyses of system attributes to optimize the RMA performance of a system within the program's operational and programmatic constraints throughout the system lifecycle. Quantitative assessments are probabilistic, mean, and/or distribution assessments; qualitative analyses are failure mode assessments. Evaluation of the design's ability to meet operational readiness requirements through preventive and corrective maintenance.
Human Factors Engineering	Multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: equipment, systems, facilities; procedures, jobs, environments; staffing; training; and Personnel and organizational management for safe, comfortable, and effective human performance.

Table 4.8-1. Specialty Engineering Disciplines—Continued

Specialty Engineering Discipline	Description
E^3	System analysis for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems, identify sources of interference, and implement methods for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards. E^3 consists of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC).
Quality Engineering	An objective analysis of all planned and systematic activities to ensure that a product or service fulfills requirements and is of the highest quality.
Information Security Engineering (ISE)	Application of scientific and engineering principles to manage and control system security risk to the enterprise and its mission. Risk identification includes identifying system vulnerabilities and threats. ISE applies effective and suitable technical, procedural, physical, and administrative controls to mitigate these risks to an acceptable level. ISE combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of information technology assets (including information).
Hazardous Materials Management/Environmental Engineering	Determination of environmental impacts at deployment sites and during operations, including both environmental impacts on the system and system impacts on the environment during all phases of the product's life.

In addition to resolving problems and defining requirements early, Specialty Engineering supplies information to the other SE functions, including Requirements Management (Section 4.3), Risk Management (Section 4.10), Configuration Management (Section 4.11), and Validation and Verification (Section 4.12). Table 4.8-2 highlights the effect that Specialty Engineering has on the other SE processes.

Table 4.8-2. Major Effects of Specialty Engineering on Other System Engineering Processes

Affected SE Process	How Affected
Integrated Technical Planning (Section 4.2)	The Integrated Technical Planning process feeds Specialty Engineering. Integrated Technical Planning produces the plans for Specialty Engineering, SE, and all other SE processes. The plans detail what is to be done, who is to do it, the standards of performance, and when each task is to be performed.
Requirements Management (Section 4.3)	The Requirements Management process both feeds and is fed by Specialty Engineering. The specialist describes the system in order to perform Specialty Engineering analyses. Requirements are a key component of any description, and they are an output of the Requirements Management process. Specialty Engineering studies often find characteristics that create a need for new or different requirements. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more requirements. In either case, the Specialty Engineering function develops the new or changed requirements, and these are an input to the Requirements Management process.
Functional Analysis (Section 4.4)	The Functional Analysis process both feeds and is fed by Specialty Engineering. To execute a Specialty Engineering analysis, the specialist shall have a thorough understanding of the system functions. This understanding is a result of performing a Functional Analysis of the system.
Interface Management (Section 4.7)	Specialty Engineering both feeds and is fed by Interface Management. The specialist describes the system to perform Specialty Engineering analyses. Interface Requirements Documents (IRD) are key components of any system description and are an output of the Interface Management process. Specialty Engineering studies often find characteristics that create a need for new or different interface requirements. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more interfaces. In either case, the Specialty Engineering function develops the new or changed requirements, which are inputs to the Interface Management process.

Table 4.8-2. Major Effects of Specialty Engineering on Other System Engineering Processes—Continued

Affected SE Process	How Affected
Risk Management (Section 4.10)	Specialty Engineering feeds the Risk Management process. Specialty Engineering studies and analyses find and assess potential problem areas of a design as early as possible. When a potential problem is found, the information becomes an input to the Risk Management process for risk mitigation and control.
Configuration Management (Section 4.11)	Specialty Engineering outputs are inputs to the Configuration Management process. In performing Specialty Engineering analyses, specialists may discover that additional or changed design features are required or that changes to operating, maintenance, or installation procedures are needed. When these discoveries occur, the proposed changes become inputs to the Configuration Management process.
Validation and Verification (Section 4.12)	Specialty Engineering outputs feed the Validation and Verification process. Early in the program's lifecycle, specialists use Specialty Engineering to validate requirements by comparing the requirements defined in early Specialty Engineering analyses to those defined in current/later analyses. If the Specialty Engineering analyses find a need for an existing requirement, then the requirement may be considered validated. Specialty Engineering feeds Verification Criteria to the Verification process. Specialists also use Specialty Engineering to verify requirements later in the system's lifecycle, either by test or SE Assessment. Specialty Engineering is a form of assessment and may be used to demonstrate verification.

4.8.0.2 Inputs and Providers to Specialty Engineering

Table 4.8-3 depicts the inputs needed to conduct Specialty Engineering analyses.

Table 4.8-3. Specialty Engineering Process Inputs

Process Input	Input Purpose/Description	From Process
FAA Policy and Standards	Policy and standards, such as the Acquisition Management System (AMS), define what is expected to be accomplished and how well it needs to be done.	AMS and FAA Orders
National Airspace System (NAS) Enterprise Architecture	The NAS Enterprise Architecture is the technical blueprint for modernizing the NAS and guides the Federal Aviation Administration (FAA) on what systems are planned for modernization.	Integrated Technical Planning (Section 4.2)
System Engineering Management Plan (SEMP)	The SEMP defines the plan for conducting SE in the AMS and a program.	Integrated Technical Planning (Section 4.2)
Requirements	Requirements provide information about the system's required characteristics, specifications, performance, and requirements. They assist in developing the system description. System requirements are documented in the preliminary Program Requirements (pPR), the final Program Requirements (fPR), and system specification(s).	Requirements Management (Section 4.3)
Requirements Verification Compliance Documents (RVCD)	The RVCD records the verification status of all requirements.	Requirements Management (Section 4.3)
Concepts	Concepts are captured in user-oriented documents that describe system functional characteristics for a proposed system from the user's viewpoint. It explains the existing system, current environment, users, interactions among users and the system, and organizational impacts. Concept documents communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements.	Functional Analysis (Section 4.4)

Table 4.8-3. Specialty Engineering Process Inputs—Continued

Process Input	Input Purpose/Description	From Process
Functional Architecture	The Functional Architecture identifies, analyzes, and describes the functions of a system. It provides information required for a system description and assists in defining requirements. Functional Analysis is a System Engineering process that takes stakeholders' needs and translates them into a sequenced and traceable functional architecture.	Functional Analysis (Section 4.4)
Operational Services and Environmental Description (OSED)	The OSED is a comprehensive, holistic system description that describes the services, environment, functions, and mechanizations that form a system's characteristics.	Functional Analysis (Section 4.4)
Description of Alternatives	Description of Alternatives conveys the various Physical Architectures being analyzed for implementation. When Trade Studies (Section 4.6) are performed, a number of alternatives shall be competitively evaluated.	Synthesis (Section 4.5)
Physical Architecture	Physical Architecture is a hierarchical arrangement of hardware and/or software components along with their associated interfaces that depicts the physical definition of the system.	Synthesis (Section 4.5)
Interface Control Document (ICD)	The ICD contains and documents the "as built" interface design derived from the IRD.	Interface Management (Section 4.7)
Analysis Criteria	Criteria for specialty engineering analyses specifically establish the degree of validation required for the analyses and associated tools, the methods for ensuring proper quality and range of data, and the level of documentation required.	Integrity of Analysis (Section 4.9)

Table 4.8-3. Specialty Engineering Process Inputs—Continued

Process Input	Input Purpose/Description	From Process
Baselines (i.e., Approved Baselines, Approved Baseline Changes, Updated Baselines)	When the requirements and design have matured sufficiently, they are baselined to facilitate management of the configuration.	Configuration Management (Section 4.11)
Validation Reports	Validation Reports document the results of the Validation effort. They report requirements that are validated and those that are considered nonconforming.	Validation (Section 4.12)
Constraints	Constraints are boundaries within which the system must remain. Risk mitigation plans often impose constraints that impact other areas of a program.	Risk Management (Section 4.10)
System Engineering Manual (SEM) Revisions	The SEM and its revisions are not direct inputs into the Specialty Engineering process. However, they do impact the actual conduct of the process. As the process is practiced, feedback from users may necessitate changes to the process. The SEM documents such changes.	System Engineering Process Management (Section 4.14)

4.8.0.3 General Specialty Engineering Process Tasks

All Specialty Engineering disciplines follow a similar process during the conduct of associated analyses. The following subsections give general guidance on performing Specialty Engineering in the FAA. These processes, as shown above in Figure 4.8-1, are the following:

- Describe the system in physical and/or functional terms. The specialists must complete this task before beginning the analysis and should use existing system descriptions if they contain enough detail. If they don't, the specialists will have to generate a description, ensuring that it adheres to the guidance in Functional Analysis (Section 4.4) and Interface Management (Section 4.7).
- Bound the problem and define Constraints on the Specialty Engineering study and the design
- Select analytical methods and tools

- Analyze system parameters to determine specialty attributes that are specific to the views of the Specialty Engineering study
- Define or assess the Specialty Engineering Requirements
- Coordinate results with stakeholders
- Document the analysis results in a Design Analysis Report (DAR)

The following subsections detail the process tasks depicted in Figure 4.8-1.

4.8.0.3.1 Task 1: Obtain or Develop an Operational Services and Environmental Description (OSED)

The first task of the specialty engineer is to understand and describe the system at an appropriate level. The OSED is an excellent source for this information, since it is a system description that is developed in the Functional Analysis process (Section 4.4).

It is recommended that the specialty engineer use the existing descriptions to frame the Specialty Engineering analysis. However, sometimes the existing system descriptions lack sufficient detail. In these cases, the specialty engineer develops the system description; and, in doing so, shall comply with the guidance in Functional Analysis (Section 4.4).

Functional Analysis describes the desired behaviors of a system. These behaviors provide critical insight into how the system is intended to perform and, therefore, are a critical input to any Specialty Engineering analysis. To perform an assessment of a system, the engineer has to understand the functions of that system and be able to relate the specialties to these functions. Normally, Functional Analysis is completed before the Specialty Engineering process begins, and the specialty engineer only has to obtain and review the Functional Analysis and use it to enhance or complete the system description. In some cases—either because the engineers failed to perform it or because it is too early in the design process—the Functional Analysis is not available. In these cases, the specialty engineer shall refer to guidance in Functional Analysis and perform the Functional Analysis independently.

4.8.0.3.2 Task 2: Bound the Problem and Define Constraints on the Study and Design

Every system problem or analysis has breadth and depth. The breadth of a system analysis refers to the system boundaries. Boundaries limit the system to elements of the system model that affect or interact with each other in order to accomplish the central mission(s) or function. Depth refers to the level of detail in the description; this level varies inversely with the breadth of the system. For a system as broad as the NAS, the description and analysis are general in nature with little detail on individual components. On the other hand, a simple system, such as a valve in a landing gear design, includes significant detail to support the assessment.

Design Constraints play an important role in conducting analysis and the credibility of the results. It is essential to identify the Constraints before the analysis to account for their influence on the methods used and the alternatives chosen. As part of determining the Constraints, the engineer identifies the scope of the analysis, the ground rules, and assumptions. Identifying the customer(s) for the analysis is important with respect to defining the scope. The analysis may be subject to contractual restraints if it is a deliverable, and the engineer has to consider these restraints when defining the scope of the effort. The project schedule and budget may also impose limits on the analysis, which may affect the assumptions and ground rules. The analysis team and the recipients of the report shall be aware of all the scope limitations, ground rules, assumptions, and guidelines that apply to the assessment and product design. The following sources are used to identify Constraints:

- Concepts defined via Functional Analysis (Section 4.4)
- Contract Statement of Work, including Work Breakdown Structure, and referenced standards and procedures
- Compliance documents that apply to the analysis methods and report
- Customer-specified requirements on cost, schedule, and product performance
- Management-imposed business goals and Constraints
- Functional, performance, and interface requirements derived from the design concept
- Functional, performance, and interface requirements imposed by use of commercially available or preexisting hardware and software
- Operational constraints imposed by the user
- Environmental constraints imposed by the physical and operational environment
- Constraints imposed by the production or Verification process (Section 4.12)
- Design constraints imposed by standard practices that are defined by the government or standards-setting bodies
- Federal, Department of Transportation, and FAA policies, standards, and guidelines

4.8.0.3.3 Task 3: Select Analytic Methods and Tools

To ensure Integrity of Analyses (Section 4.9), the engineer selects analytic methods and tools that meet the program phase requirements; the system analysis needs; and cost, schedule, and skill constraints. It is important to select methods and tools that match the analysis objectives within the resource limitations of the effort.

4.8.0.3.4 Task 4: Analyze System Parameters To Determine System Attributes

In this step, engineers use the methods and tools appropriate to the Specialty Engineering discipline to determine the attributes of the design. For some analyses, it is recommended that the results include programmatic attributes, such as cost and schedule impacts, as appropriate to the analysis. Table 4.8-4 lists the appropriate guidelines and handbooks for each Specialty Engineering discipline. The AMS FAA Acquisition System Toolset (FAST) often contains guidelines for these activities, such as the FAA System Safety Handbook (SSH) and the Safety Risk Management Guidance for System Acquisistion (SRMGSA).

In addition, as part of this process, technical or peer reviews of the analysis and its results are conducted. The technical community conducts this independent evaluation before the Specialty Engineering DARs are submitted.

The results of Specialty Engineering analyses confirm design attributes necessary for acceptable product performance, cost, schedule, and risk. When an attribute is not confirmed, the analysis and/or the baseline shall be revised.

Revision may be implemented through changes in scope, ground rules, assumptions, and analytic methods. The analysis process is reactivated to determine an alternative result that is acceptable and valid. Alternatively, the results of the analysis may drive revision of the Requirements or design baseline. This revision is accomplished by preparing appropriate change proposal documentation for input to the Configuration Management process (Section 4.11).

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering

Phase	Analysis	Guidelines and References
Mission Analysis	E^3 EMC requirements	FAST. (2000). Environment/Energy/Safety/Health. http://fast.faa.gov/ FAST. (2000). Radio Spectrum Management. http://fast.faa.gov/
	Environmental Requirements Analysis	FAST.[1] Environment/Energy/Safety/Health. http://fast.faa.gov/
	Human Factors System (Mission) Analysis	FAST. Human Factors. http://fast.faa.gov/
	Human Factors Requirements and Functional Analysis	FAST. Human Factors. http://fast.faa.gov/
	Maintainability Requirements Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Operational Safety Assessment	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH[2], Chapter 4 SRMGSA[3], Chapters 3 and 4

[1] Federal Aviation Administration, Federal Acquisition System Tools (FAST), ATO, [On-line] Available: http://fast.faa.gov.

[2] U.S. Federal Aviation Administration, "FAA System Safety Handbook," ATO Safety Office (ATO-S), Washington, DC (2000).

3 U.S. Federal Aviation Administration, "NAS Modernization System Safety Management Plan, ATO Safety Office (ATO-S), Washington, DC (2000).

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering—Continued

Phase	Analysis	Guidelines and References
	Information Security Engineering	Preliminary Risk Assessment, Guidance/Reference: FAA ISS Handbook 1370.82
Investment Analysis	Comparative Safety Assessment	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 4 SRMGSA
	EMC Control Plan	FAST. (2000). Environment/Energy/ Safety/Health. http://fast.faa.gov/ FAST. (2000). Radio Spectrum Management. http://fast.faa.gov/
	Human Factors Program Plan	FAST. Human Factors. http://fast.faa.gov/
	Maintainability Plan	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Preliminary Hazard Analysis	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 SRMGSA
	Quality Engineering Plan	FAST. Quality Assurance. http://fast.faa.gov/
	Specialty Engineering Support of Trade Studies or Alternatives Analysis	FAST. Investment Analysis. http://fast.faa.gov/ Synthesis of Alternatives (Section 4.5)
	System Safety Program Plan	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 5 SRMGSA
	Information Security Engineering	Updated Risk Assessment, Guidance/Reference: FAA ISS Handbook 1370.82

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering—Continued

Phase	Analysis	Guidelines and References
Solution Implementation	Environmental/ Hazardous Material Analysis	FAST. Environment/Energy/Safety/Health. http://fast.faa.gov/
	Failure Modes and Effects Analysis	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 SRMGSA
	Failure Modes and Effects Criticality Analysis	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 SRMGSA
	Hazard Tracking and Risk Resolution	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 3 SRMGSA
	Human Factors Demonstrations, Models, Simulations, and Mockups	FAST. Human Factors. http://fast.faa.gov/
	Human Factors Operator/Maintainer/ Supervisor Cognitive Task and Workload Analysis	FAST. Human Factors. http://fast.faa.gov/
	Human Factors Personnel, Staffing, and Training Analysis	FAST. Human Factors. http://fast.faa.gov/
	Human Factors Performance and Error Analysis	FAST. Human Factors. http://fast.faa.gov/
	Maintainability Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintainability Demonstration	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintainability Modeling	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintenance Task Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Operating and Support Hazard Analysis	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 SRMGSA

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering—Continued

Phase	Analysis	Guidelines and References
	Subsystem Hazard Analysis	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 SRMGSA
	System Hazard Analysis	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 SRMGSA
	Information Security Engineering	Analysis supporting Certification and Authorization, Guidance/Reference: FAA ISS Handbook 1370.82

4.8.0.3.5 Task 5: Define and Document Specialty Engineering Requirements

The attributes developed in “Task 4: Analyze System Parameters To Determine System Attributes” (subsection 4.8.0.3.4) are used to define Specialty Engineering-related requirements. These requirements shall meet the standards for requirements definition and documentation described in Requirements Management (Section 4.3). In addition, these requirements shall be validated and verified, as described in Validation and Verification (Section 4.12).

4.8.0.3.6 Task 6: Coordinate Results With Stakeholders

The results of the Specialty Engineering process (particularly the DARs and Requirements) shall be coordinated with the project/program stakeholders in both formal and informal forums. The informal forums include peer reviews and working groups. The formal forums include Acquisition Reviews and Design Reviews, as described in Integrated Technical Planning (Section 4.2).

4.8.0.3.7 Task 7: Document the Specialty Engineering Analysis in a Design Analysis Report

The DAR is the primary output of any Specialty Engineering function. It documents the results—including the rationale—of the specific analysis. Each DAR shall contain the following results:

- Description of the system's special characteristics
- List of existing Requirements that were either validated or verified in the analysis
- Residual risks
- Candidate Requirements found as a result of the analysis

These DAR requirements are inputs to the Requirements Management process (Section 4.3) and shall be considered for inclusion in the preliminary Program Requirements (pPR) and the final Program Requirements (fPR). The rationale includes the scope, ground rules, assumptions, constraints, methods, and tools applicable to the analysis.

Specialty Engineering outputs are often used to validate and/or verify requirements. In addition, change proposal documentation is produced if the conclusions of the analysis call for a revision to the Requirements or design baseline. This revision is an input to the

Configuration Management process (Section 4.11) for authorization to change the baseline as the analysis indicates.

Requirements for contents and format may be applicable to the DAR as specified by the contract. Figure 4.8-2 is a sample outline of the DAR contents.

1.0 Executive Summary
2.0 Introduction
3.0 Summary of results
4.0 Summary of conclusions (including residual risks)
5.0 Recommendations (including mitigation)
6.0 System Description
   6.1 Summary
   6.2 Operational Services and Environment Description (OSED)
   6.3 Functional Analysis (if applicable)
   6.4 Requirements (if applicable)
7.0 Description of system special characteristics (detailed analysis worksheets or data)
8.0 List of candidate requirements
9.0 List of requirements that were validated and/or verified with rationale
10.0 Analysis methodology with rationale

Figure 4.8-2. Sample Outline of a Design Analysis Report

4.8.0.4 Outputs of Specialty Engineering

These are the Specialty Engineering outputs, which are described in subsequent subsections.

- Security Certification and Authorization Package
- Planning Criteria
- DARs (specific to the Specialty Engineering study)
- Constraints
- Tools/Analysis Requirements
- Concerns and Issues
- Verification Criteria

4.8.0.4.1 Security Certification and Authorization Package

For certification information, see subsection 4.8.6.

4.8.0.4.2 Planning Criteria

Any Planning Criteria needed to perform Specialty Engineering throughout the remainder of the program's lifecycle is provided to the Integrated Technical Planning process (Section 4.2).

4.8.0.4.3 Design Analysis Report

The DAR documents and reports the methods and results of the Specialty Engineering analyses. Figure 4.8-2 (above) provides a sample outline of a DAR. In performing an analysis, the specialty engineer typically defines, refines, or validates requirements. Occasionally, the specialist discovers system characteristics that are not adequately specified in the existing requirements or specification documents. In these cases, the specialist defines or modifies those requirements in the DAR to be consistent with the specialist's area of expertise and the requirements standards described in Requirements Management (Section 4.3).

4.8.0.4.4 Constraints

Constraints for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Trade Studies process (Section 4.6).

4.8.0.4.5 Tools/Analysis Requirements

Tools/Analysis Requirements for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Integrity of Analyses process (Section 4.9).

4.8.0.4.6 Concerns and Issues

Appendix D contains guidance on Concerns and Issues as a product of Specialty Engineering.

4.8.0.4.7 Verification Criteria

The specialist may be asked to define specific verification requirements, as described in "Step 3: Develop Verification Approach" in Section 4.12 (subsection 4.12.2.5.2.2.3). The Verification Criteria or requirements are added to the Verification Requirements Traceability Matrix (VRTM).

4.8.0.5 Specialty Engineering Tools

Each Specialty Engineering discipline often uses unique Specialty Engineering tools. They include databases, drawing tools, requirements and Functional Analysis tools, word and document processors, and spreadsheets. Selection of specific tools depends on criteria established by the particular program. These tools are identified and controlled as documented in appropriate program planning documents.

4.8.0.6 Specialty Engineering Process Metrics

The extent of progress being made in completing the Specialty Engineering analyses, as compared with the program's plans for conducting such analyses, is a measure of the degree to which these analyses are being effectively managed. The effectiveness of Specialty Engineering analyses may be measured by the extent of rework of analyses or incompatibility of analyses with measured performance, indicating that the analyses are reaching inaccurate conclusions.

Additional candidate metrics that measure the overall process and products of Specialty Engineering include:

- Percent of validated assumptions pertaining to the DAR
- Percent of validated Specialty Engineering requirements recommended in the DAR
- Percent of verified Specialty Engineering requirements recommended in the DAR
- Percent of open concerns and issues that have been identified as a result of the Specialty Engineering process

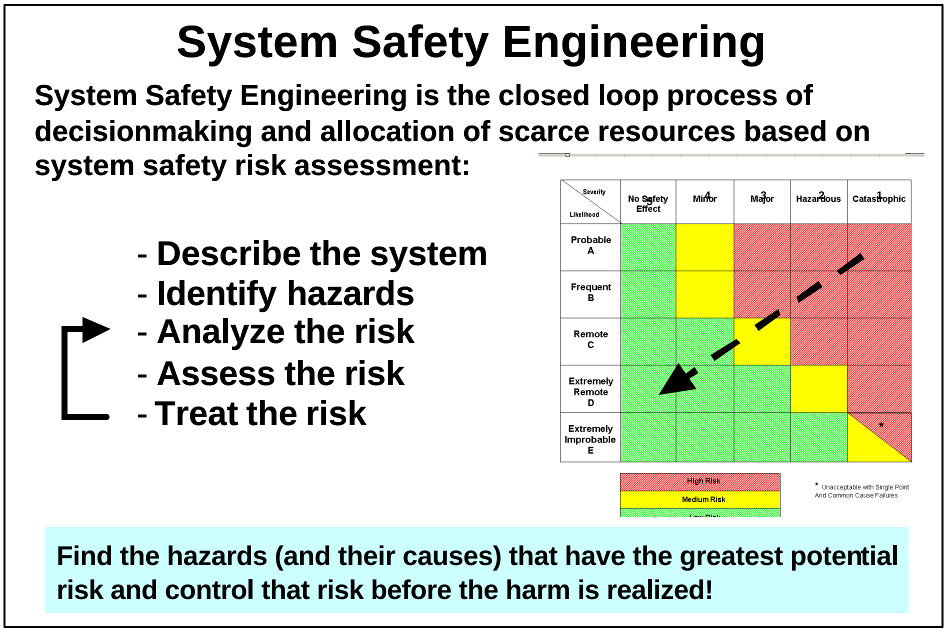
4.8.1 System Safety Engineering

System Safety Engineering (SSE) is a Specialty Engineering discipline within SE. It is recommended that system/safety engineers and program managers refer to the FAA's Safety Management System (SMS) Manual, the Safety Risk Management Guidance for System Acquisition (SRMGSA), and the FAA's System Safety Handbook (SSH) for detailed information for planning and conducting SSE. The following paragraphs describe how system safety is integrated into a system's overall SE.

4.8.1.1 What Is System Safety Engineering?

SSE is the application of engineering and management tools—including principles, criteria, and techniques—to optimize the safety of a system within the program's operational and programmatic constraints. These tools are used to identify, evaluate, and control hazards associated with a system. A hazard is any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment. SSE's goal is to identify the hazards in a system early, to continuously assess the risk (severity and likelihood) of each hazard, and to actively control the highest risk hazards. The SRMGSA (http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm) provides more information on this topic.

As illustrated in Figure 4.8.1-1, the SSE process is a closed-loop method of Risk Management (Section 4.10).



System Safety Engineering

System Safety Engineering is the closed loop process of decisionmaking and allocation of scarce resources based on system safety risk assessment:

- Describe the system
- Identify hazards
- Analyze the risk
- Assess the risk
- Treat the risk

Severity / Likelihood	5 No Safety Effect	4 Minor	3 Major	2 Hazardous	1 Catastrophic
Probable A	🟩	🟨	🟥	🟥	🟥
Frequent B	🟩	🟨	🟥	🟥	🟥
Remote C	🟩	🟩	🟨	🟥	🟥
Extremely Remote D	🟩	🟩	🟩	🟨	🟥
Extremely Improbable E	🟩	🟩	🟩	🟩	🟥 * 🟨

🟥 High Risk
🟨 Medium Risk
🟩 Low Risk

* Unacceptable with Single Point And Common Cause Failures

Find the hazards (and their causes) that have the greatest potential risk and control that risk before the harm is realized!

Figure 4.8.1-1. Closed-Loop Nature of System Safety Engineering

The following documents describe how SSE is conducted in the AMS:

- Chapter 4 of the FAA's SMS Manual
- Chapter 4 of the SRMGSA (http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm)
- Chapter 8 of the FAA SSH (http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm)

Figure 4.8.1-2 shows what safety analyses are performed relative to the phases of the AMS. The analyses are timed to best support the phased needs and decisions in the overall AMS process.

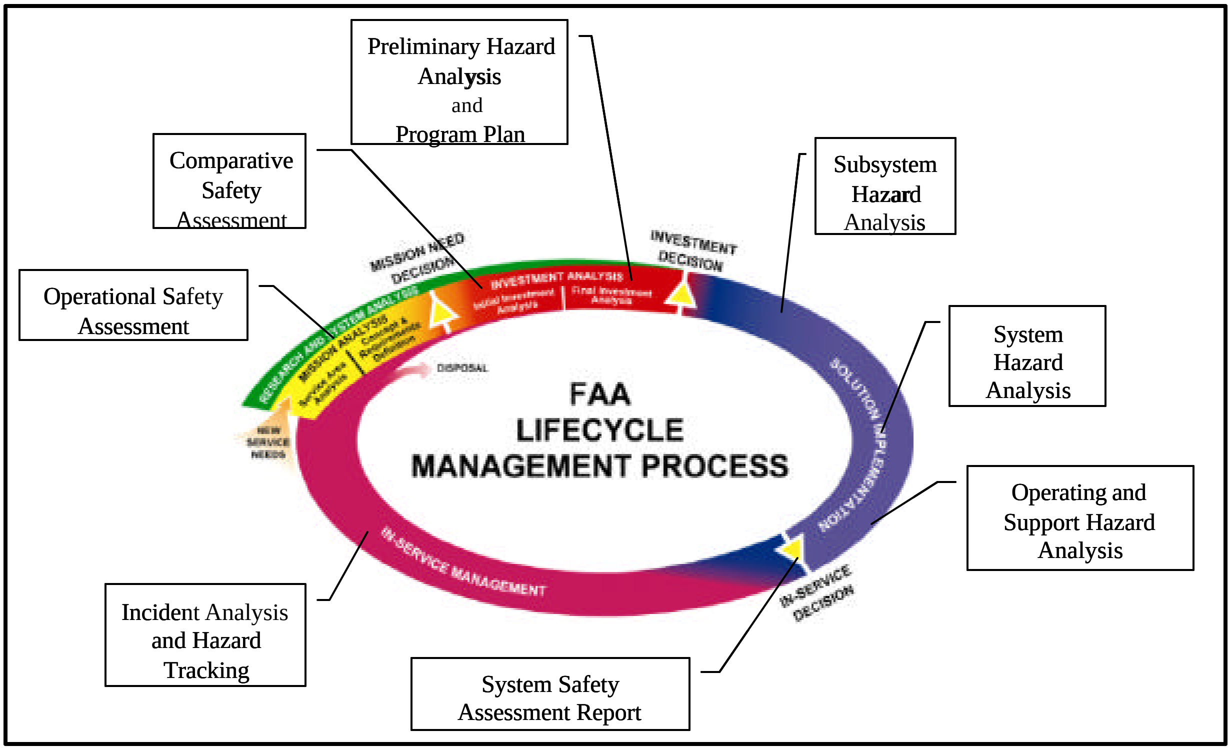
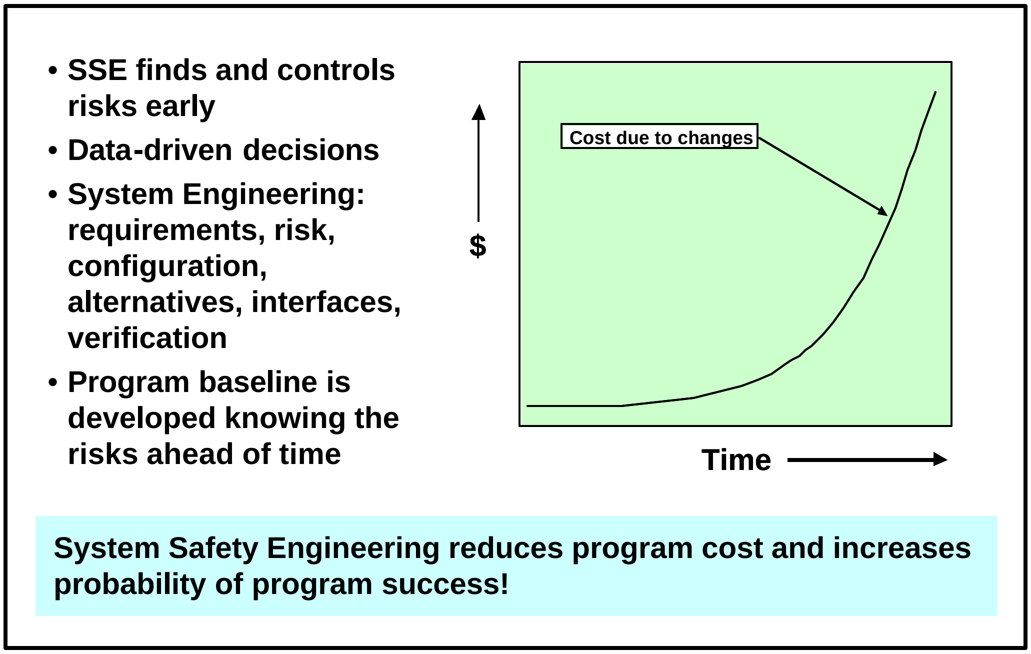

Preliminary Hazard Analysis and Program Plan
Comparative Safety Assessment
Subsystem Hazard Analysis
Operational Safety Assessment
System Hazard Analysis
Operating and Support Hazard Analysis
Incident Analysis and Hazard Tracking
System Safety Assessment Report
MISSION NEED DECISION
INVESTMENT DECISION
INVESTMENT ANALYSIS
Initial Investment Analysis
Final Investment Analysis
RESEARCH AND SYSTEM ANALYSIS
MISSION ANALYSIS
Service Area Analysis
Concept & Requirements Definition
NEW SERVICE NEEDS
DISPOSAL
FAA LIFECYCLE MANAGEMENT PROCESS
SOLUTION IMPLEMENTATION
IN-SERVICE DECISION
IN-SERVICE MANAGEMENT

Figure 4.8.1-2. Types of Safety Hazard Analyses and Their Relative Position in the Acquisition Management System

4.8.1.2 Why Perform System Safety Engineering?

Performing SSE on a program optimizes the safety of a system by identifying, evaluating, and controlling hazards. SSE is also performed to:

- **Comply with FAA orders, the SMS, and AMS direction.** The FAA's primary role is to ensure the safety of the NAS. Thus, the FAA has issued FAA Order 8040.4, which directs all FAA organizations to employ safety risk management in decision making. The safety risk management sections of the FAA's SMS Manual present the methodology to comply with the order. Additionally, AMS policy, in accordance with FAA Order 8040.4, requires programs to perform system safety and to brief the system safety program status at all decision points and investment reviews. The SSH, the SRMGSA, and the AMS provide more information on this subject (http://fast.faa.gov/toolsets/SafMgmt/IndexStart.htm).
- **Reduce total cost of development.** SSE reduces cost and improves system integration and SE overall. SSE looks for programmatic risks that may impact system performance, schedule, and costs and finds problems early. As Figure 4.8.1-3 shows, the earlier in the lifecycle a problem is found and managed, the easier and less expensive it is to correct.
- **Improve program integration.** Outputs of the system safety process feed other SE processes, which improves the system's overall SE (Figure 4.8.1-4).



- SSE finds and controls risks early
- Data-driven decisions
- System Engineering: requirements, risk, configuration, alternatives, interfaces, verification
- Program baseline is developed knowing the risks ahead of time

System Safety Engineering reduces program cost and increases probability of program success!

Figure 4.8.1-3. Benefits of System Safety Engineering

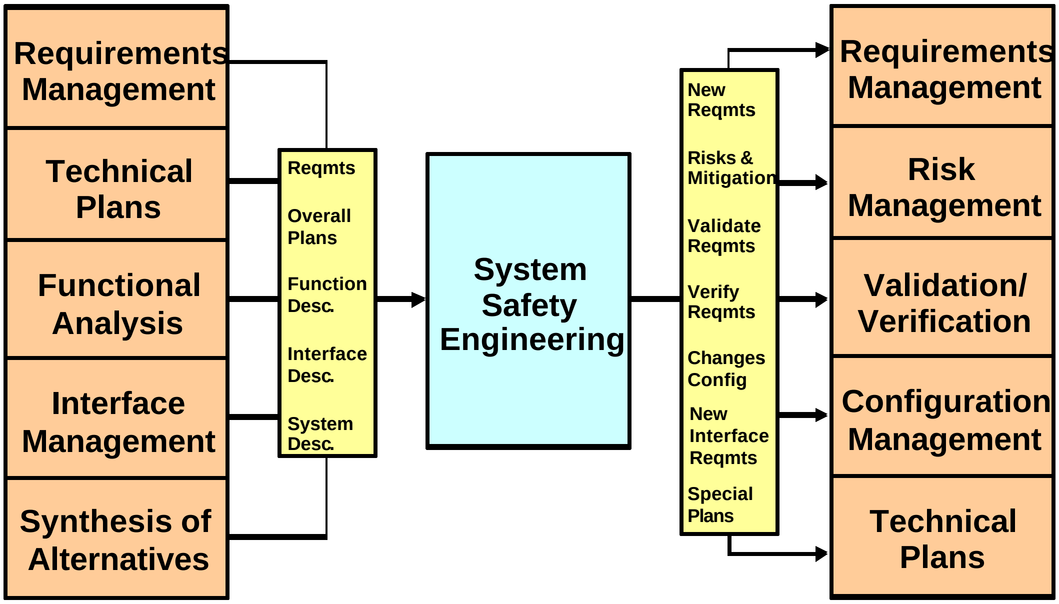


Figure 4.8.1-4. System Safety Engineering's Relationship to Other System Engineering Processes

4.8.1.2.1 System Safety Engineering Process Tasks

SSE follows the process tasks outlined in "General Specialty Engineering Process Tasks" (subsection 4.8.0.3). These general tasks correlate directly with the specific SSE tasks in Table 4.8.1-1 and, as previously stated, appear in the FAA's SMS Manual and SSH and the NAS SSMP.

Table 4.8.1-1. General Specialty Engineering Tasks Correlated to SSE Tasks

General Specialty Engineering Process Tasks	Specific SSE Process Tasks
Obtain or develop an OSED	**Describe the system** 1. Describe the system or operation that is being added or changed 2. Plan the safety risk-management effort (define scope and objectives; identify stakeholders)
Bound the problem and define Constraints on the study and design	
Select analytical methods and tools	
Analyze system parameters to determine system attributes	**Identify hazards** 3. Identify the hazards 4. Identify hazard causes
	Analyze the risk 5. Assess the risk of the hazards (i.e., severity and likelihood) 6. Analyze existing controls
	Assess the risk 7. Rank hazards 8. Prioritize hazards
Define and document Specialty Engineering requirements	**Treat the risk** 9. Define risk-management strategies 10. Select risk-management strategies 11. Implement risk-control strategies 12. Verify control strategies through monitoring and tracking
Coordinate results with stakeholders	
Document the Specialty Engineering analysis in a DAR	

4.8.1.3 System Safety Engineering Outputs and Products

The following products are SSE outputs.

4.8.1.3.1 Program Planning

Each program has to have a Program Safety Plan (PSP) per the SRMGSA, which is the overall plan for conducting system safety management in the AMS. It is recommended that individual programs, when developing a program-specific PSP, consult the SRMGSA, which also develops the requirements for the vendor's or contractor's System Safety Program Plan (SSPP). The FAA SSH, Chapter 5 (http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm), also provides guidance on this topic.

4.8.1.3.2 Analysis Products

Table 4.8.1-2 lists the SSE products and detailed directions on how to develop them.

Table 4.8.1-2. Products of System Safety Engineering

System Safety Process Products	How To Reference
Operational Safety Assessment (OSA)	FAA SSH, Chapters 2 and 4 (http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm) SRMGSA, Section 5.2.1 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.1)
Comparative Safety Assessment (CSA)	FAA SSH, Chapters 2 and 4 SRMGSA, Section 5.2.2 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.2)
Preliminary Hazard Analysis (PHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.3 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.3)
Integrated Safety Plan (ISP)	SSMP, Section 5.2.4 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4)
System Safety Program Plan (SSPP)	FAA SSH, Chapter 5 SRMGSA, Section 5.2.4 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4)
Subsystem Hazard Analysis (SSHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.5 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.5)

Table 4.8.1-2. Products of System Safety Engineering—Continued

System Safety Process Products	How To Reference
System Hazard Analysis (SHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.6 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.6)
Operating and Support Hazard Analysis (O&SHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.7 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.7)
Health Hazard Assessment (HHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.8 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.8)
System Safety Assessment Report (SSAR)	SRMGSA, Section 5.2.10 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10)
Hazard Tracking Risk Resolution System (HTRR)	FAA SSH, Section 2.2.3 SRMGSA, Section 5.2.11 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.11)
Safety Requirements Verification Table (SRVT)	SRMGSA, Section 5.2.12 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.12)

4.8.2 Reliability, Maintainability, and Availability Engineering

This section provides guidance to facilitate, manage, and coordinate Reliability, Maintainability, and Availability (RMA) efforts, which ensure operationally acceptable RMA characteristics in fielded systems.

4.8.2.1 What Is RMA Engineering?

RMA Engineering applies engineering and management principles, criteria, and techniques to optimize the RMA performance of a system within the program's operational and programmatic constraints throughout the system lifecycle. These engineering and related management tools are used to identify, evaluate, and control RMA characteristics associated with a system. Thus, RMA Engineering primarily minimizes the probability of system failure and any potential losses stemming from such failure. RMA accomplishes this by establishing RMA requirements, assessing system RMA attributes, and analyzing solutions developed to meet established RMA requirements within realistic cost constraints.

4.8.2.1.1 RMA Detailed Definitions

The following detailed RMA definitions provide background and context for the subsequent RMA Engineering discussions:

- *Reliability* quantifies a system's ability to perform without failure
- *Maintainability* quantifies a system's ability to recover from failure
- *Availability* quantifies a system's ability to perform when needed

4.8.2.1.1.1 Reliability

Reliability is the ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system. It is generally characterized by the Mean Time Between Failures (MTBF). Quantitatively, this translates to the probability that a system or constituent piece may perform a required function under specific conditions for a stated period of time. The formula in Equation 1 calculates Reliability.

$$R(T_2 - T_1) = e^{-\int_{T_1}^{T_2} h(t)\,dt}$$

Equation 1. Reliability Formula

where:

- $R(T_2 - T_1)$ is the *Reliability*, or probability that the system will not fail during the interval from time T_1 to T_2, assuming no failure at T_2, and
- h(t) is the *Hazard Rate*, or average rate of failure per hour experienced over specified small time intervals (e.g., 1 hour)

Whereas hazard rates are measured over small intervals of time (e.g., 1-hour periods), another useful metric for reliability characterization is the *Failure Rate*, which is the average hazard rate per hour, averaged over a given period of operating time, as follows:

$$l\,(T_2 - T_1) = \frac{\int_{T1}^{T2} h(t)dt}{T_2 - T_1}$$

where:

- $\lambda\ (T_2 - T_1)$ is the failure rate from time T_1 to T_2

Another reliability parameter is the *Mean Time To Failure* (MTTF), which is the average time for a system to fail initially, based on the behavior of similar systems, operated under specified conditions for the duration of a specified time interval. It is related to the failure rate of the system as follows:

$$MTTF\,(T_2 - T_1) = \frac{1}{l\,(T_2 - T_1)}$$

The above equations show that the three fundamental parameters defined include time-based dependencies. This implies nonlinear complexities when component reliability values are aggregated to characterize the reliability of the system they comprise. However, during the operational phase of deployed system, hazard rates tend to maintain a constant value, especially at the component level. This assumption allows use of the following simplified relationships and parameters:

$$l\,(T) = h(t) = l$$

that is, the hazard rate is equal to the failure rate, which is constant over time, and,

$$MTBF = MTTF = \frac{1}{l}$$

where MTBF is the Mean Time Between Failures, the basic measure of reliability for repairable systems or constituent pieces with time-constant hazard rates. MTBF is the mean number of life units during which all parts of the system or constituent pieces perform within their specified limits, during a particular measurement interval under stated conditions. Equation 2 calculates MTBF.

$$MTBF = \frac{T}{F}$$

Equation 2. MTBF Formula

where:

- *T* is the duration of the measurement interval
- *F* is the number of failures that occurred during the measurement interval

4.8.2.1.1.2 Maintainability

Maintainability is the measure of the ability of a failed system or constituent piece to be restored to full operational status. It is generally characterized by the Mean Time To Restore (MTTR), which is the average total elapsed time from initial failure to resumption of operation. MTTR includes *all* downtime, including the average time to obtain spares and appropriate personnel to begin the repair (i.e., Mean Logistic Delay Time) and the time to repair and restore the system. It is expressed as the sum of the logistic delay, corrective diagnosis, and maintenance times, divided by the total number of failures of a system or constituent piece. (see Equation 3). MTTR is usually expressed in hours.

$$MTTR = \sum_{t=1}^{F_T} \frac{LogisticDelay_t + \mathrm{Diagnosis}_t + \mathrm{Maintenance}_t}{F_T}$$

Equation 3. MTTR Formula

where:

- *t* is an integer representing an occurrence requiring corrective diagnosis and associated corrective maintenance
- *T* is the duration of the measurement interval
- F_T is the number of failures that occurred during the measurement interval
- LogisticDelay_t is the time to gather spare parts, equipment, and appropriate personnel to begin the repair
- Diagnosis_t is the time to perform corrective diagnosis
- Maintenance_t *is the time to perform corrective maintenance*

Maintainability requirements generally pertain to inherent characteristics of the system design (e.g., the ability to detect, isolate, access, and replace the failed component). In addition, a key characteristic to be addressed is any maintenance agreement for the system (e.g., warranties, incentives, and level of maintenance involved). System characteristics are generally fixed for commercial-off-the-shelf (COTS) components but may be specified, provided they do not conflict with the FAA's preference to employ COTS-based solutions whenever feasible.

4.8.2.1.1.3 Availability

Availability is the probability that a system or constituent piece will be operational during any randomly selected period of time or, alternatively, the fraction of the total available operating time that the system or constituent piece is operational. From a service perspective, availability is the percentage of time within any given interval that the service is provided to the expected level of performance specified within the target domain. Availability is appropriate as a top-level operational requirement because it is a quantitative and consistent way of summarizing the need for continuity of NAS services. Use of availability requirements may facilitate comparison and assessment of architectural alternatives. Availability is also useful as a performance metric for operational systems. Measured as a probability, availability may be defined in several ways, which allows a variety of issues to be addressed appropriately, including:

- **Inherent Availability**. This availability strictly represents the theoretical maximum availability based only on reliability (MTBF) and maintainability (MTTR). It only includes availability of the hardware components of the system. These are the only components that you can predict. Any other effects have to be measured and are included in other availability measures. The availability requirement associated with the highest criticality service supplied by the system is used to specify the inherent availability of the system. The only purpose for imposing an inherent availability requirement is to ensure that proposed constituent pieces of the system are theoretically capable of meeting a higher level requirement, based on the reliability and maintainability characteristics of these constituent pieces and the redundancy provided.

- **Equipment and Service Availability**. This availability includes all causes of unscheduled downtime. It takes into account additional downtime incurred during the failover to redundant systems or downtime incurred by other practical issues associated with unscheduled outages.

- **Operational Availability**. This availability includes scheduled and unscheduled downtime. Unlike inherent availability, operational availability includes the effects of scheduled downtime, shortages of spares, unavailable service personnel, or poorly trained service personnel. For systems or constituent pieces employing redundant elements, perfect recovery is assumed. Downtime occurs only if multiple failures within a common timeframe result in outages of the system or one or more of its pieces to the extent that the need for redundant resources exceeds the level of redundancy provided.

4.8.2.2 Why Perform RMA Engineering?

RMA directly impact both operational capability and lifecycle costs and, therefore, are important considerations in any system engineering effort. A system's ability to successfully fulfill its mission need directly depends on its ability to perform the required function under specific conditions for a given period of time without failure (reliability). Likewise, a system's operational success also depends on its ability to recover from a failure in a timely and efficient manner (maintainability). Operational success also depends on the system being ready to accomplish its mission as needed (availability). Operational and support costs for a system are predominant variables of its overall lifecycle cost. A major driver for these costs is the quality of a system's RMA characteristics. For example, redundancy is the simplest way to increase availability, although the overall system lifecycle cost increases.

To effectively and successfully coordinate RMA Engineering efforts and optimize the quality of a system's RMA characteristics, one must focus on the following objectives throughout the lifecycle of a system:

- Identify all system RMA functions, including all operational and maintenance support drivers; comprehensively incorporate RMA principles into the system requirements and design; and minimize and control the system lifecycle costs

- Measure, predict, assess, and report system trends throughout the system's lifecycle to continuously ascertain that RMA performance requirements are being met

- Achieve RMA performance objectives at all system levels

- Emphasize continuous RMA improvement

4.8.2.2.1 RMA Issues

In specifying availability, the steady state constant value (which characterizes the system availability in the long term) is not sufficient as the primary RMA requirement because it implies a tradeoff between reliability and maintainability. For example, a 1-hour interruption of a critical service that occurs annually is apparently equivalent to 240 15-second interruptions of the same service, since both scenarios provide the same availability. However, short interruptions lasting seconds are less likely to affect air traffic control operations than long interruptions lasting 1 hour or more, which may have a significant impact on traffic flow and operational safety. To address this issue, use both a steady state constant value and a dynamic expression of the system availability [A(T)], which describes the proportion of time that a system is expected to be fully functional over a specified time interval T (e.g., for the next 100 hours of operation). This metric can be used to assess availability performance over smaller bounds of time to hone in on the expectation for short interruptions in service.

In addition, availability cannot be measured as an instantaneous parameter value of a system. During system development and deployment, it may be aggregated using standardized models along with input from observable data as the system accumulates test and operations time. Demonstrations may also be performed to determine system compliance with RMA requirements. However, these activities require thorough planning of time, resources, and approach objectives to adequately capture system RMA characteristics with acceptable confidence and risk from the customer and vendor perspectives. For these reasons, one must structure and perform a rigorous RMA Engineering effort to establish detailed RMA requirements that may be monitored and verified during system development and deployment. For more quantitative details for calculating availability, see subsection 4.8.2.6 (RMA Tools).

4.8.2.3 RMA Inputs

Inputs to the RMA Engineering process include FAA Policy, standards, NAS Enterprise Architecture, SEMP, RVCD, Concepts, OSED, Interface Control documents, requirements, descriptions of alternatives, and functional and physical architectures, as well as specific measurements and other data that may be used to analyze system performance in the interrelated RMA areas (see Table 4.8-3). The inputs used within the RMA Engineering process shall be sufficient to enable computation of the required RMA characteristics (e.g., MTBF and MTTR) and comprehensive enough to conduct the appropriate analysis.

4.8.2.4 RMA Process Tasks

RMA Engineering follows the process tasks outlined in "General Specialty Engineering Process Tasks" (subsection 4.8.0.3 above). The application of an RMA program generally follows the tasks described below.

4.8.2.4.1 Task 1: Obtain an Operational Services and Environmental Description

Subsection 4.8.0.3.1 generically defines this task. Although it is useful to become familiar with the full Functional Analysis description of the target system, one should focus particularly on the failure mode and maintenance aspects, as extracted from the OSED. This information is a primary input for the RMA study efforts.

4.8.2.4.2 Task 2: Bound the Problem and Define Constraints on Studies and Design

Subsection 4.8.0.3.2 describes the generic aspects of this task. Subsection 4.8.2.3 (RMA Inputs) enumerates the sources of information used in developing the study constraints. Concerns that are of specific interest for defining the scope of RMA studies include:

- Reliability requirements needed
- System complexities that might mandate need for extreme parts control or a need for unique design tolerance
- Design concepts that might result in need for application of new or immature technology
- Applicability of parts control policies
- Logistics and support policies and plans
- Design guidelines
- Special requirements, if any, for tests
- Special facilities needed to perform tests
- Applicability of warranties, guarantees, and incentives
- Potential reliability problems based on past experiences

4.8.2.4.3 Task 3: Select Analytic Methods and Tools

Subsection 4.8.0.3.3 generically describes this task. Specifically, RMA-related tools to be considered include:

- **Design Reviews.** Scheduling of Design Reviews of the system should be based on system complexity, such as scheduling more frequent, intensive reviews during the higher risk phases of the lifecycle.
- **Failure Reporting Analysis Corrective Action System (FRACAS).** Tracking, analyzing, and correcting problems are key activities of an RMA program. The scope of

this activity should be based on system complexity and maturity, environmental constraints, testing regimen, definition of reportable failures, and organizational roles within the FRACAS. Further details on FRACAS appear below in subsection 4.8.2.5.1.3.1.

- **Reliability Modeling.** The scope of this effort depends on many factors, including system complexity, modes of system operation, environmental constraints, maintenance philosophy, and rigor of analysis.

- **Reliability prediction.** The scope of this effort depends on the quality and quantity of historical data that is available for the system and its components; granularity of analysis (e.g., subsystem or component level); and use of results (e.g., logistics modeling, and design tradeoffs).

- **Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Criticality Analysis (FMECA).** The scope of this effort depends on system complexity, subsystem and external interfaces, and new design elements. The effort also impacts maintainability, testability, logistics, and safety analyses. Details of this tasking appear below in subsection 4.8.2.5.2.1.

- **Sneak Circuit Analysis.** This task identifies latent paths that could cause undesirable behavior or inhibit desired behaviors. The task becomes more significant for analyzing critical system components and tightly coupled interfaces, or when there are frequent design changes. This effort may benefit from integration with the FMECA tasking.

- **Components Tolerance Analysis.** This task is relevant where it is important to qualify the system or its components to remain within acceptable tolerances throughout its service life.

- **Parts selection/application.** Quantity and characteristics (e.g., COTS, reliability) of procured parts and their logistical deployment affect system reliability and maintainability.

- **Environmental Stress Screening (ESS).** For less mature products, this task shakes out manufacturing defects before a program fields the system.

- **Reliability Growth Program.** This is an ongoing effort to aggregate reliability statistics as the system accumulates test and operational time. The statistics are used to infer reliability improvement as the system experiences corrective actions. Further details on the Reliability Growth Program appear below in subsection 4.8.2.5.1.3.2.

- **Reliability Qualification Tests.** These tests are performed toward the end of the Solution Implementation phase to demonstrate compliance with RMA requirements before production. The task is more significant for less mature products or products that are to be operated in conditions different from those for which they were designed.

- **Field Reliability Acceptance Tests (FRAT).** These tests ensure that system reliability as demonstrated or expected at the end of the Solution Implementation phase has not been degraded in the In-Service Management phase.

4.8.2.4.4 Task 4: Analyze System Parameters to Determine System Attributes

Subsection 4.8.0.3.4 generically describes this task. Application of RMA tools and analyses in this phase (as chosen from those described in subsection 4.8.2.6) produces system characteristics that are used as a basis for RMA requirements definition.

4.8.2.4.5 Task 5: Define and Document Specialty Engineering Requirements

Subsection 4.8.0.3.5 generically describes this task. Regarding RMA, unambiguous and measurable system RMA requirements are identified and documented based on the mission need. For example, these may be formulated as either of the following:

- A requirement with specific reliability numbers at the system or component level, at a high enough level to enable cost-effective design. An example: “The item shall have a minimum MTBF of 1,000 hours under a specified set of operating conditions.”

- An operationally based reliability requirement, as in: “The system shall be able to operate 120 days without a system-inhibiting failure.”

In addition to defining traditional RMA requirements, the program office may stipulate warranties, guarantees, and incentives to share risk and extend commitment from the vendor regarding the deployed system. There are many options to structuring these agreements; it is recommended that this be done in consultation with the Contracts support group.

4.8.2.4.6 Task 6: Coordinate Results With Stakeholders

Subsection 4.8.0.3.6 generically describes this task. Specifically, RMA objectives are not achieved independently of other program or project goals; so it is important to interface and coordinate with other stakeholder organizations to provide the proper context for RMA objectives. For example, as mentioned above, consideration of warranties must be coordinated with the relevant Contracts group. Other issues that could involve organizational coordination include planning and scheduling, test site arrangements, design reviews, subcontractor arrangements, system inspections, and corrective action procedures. Additional provisions must be made to coordinate with system-user representatives and system engineering groups to address logistics, maintainability, safety, and testing constraints.

4.8.2.4.7 Task 7: Document the RMA Analysis in a Design Analysis Report

Subsection 4.8.0.3.7 generically describes this task, and subsection 4.8.2.5.2 describes content specific to RMA studies.

4.8.2.5 RMA Outputs

Figure 4.8-1 (at the beginning of Section of 4.8) lists the various outputs that may result from performing Specialty Engineering. The following subsections detail some of these outputs as they relate to RMA Engineering.

4.8.2.5.1 Planning Criteria

The application of an RMA program generally follows the steps below. These steps shall be considered in providing planning criteria input to SE Integrated Technical Planning (Section 4.2) for the RMA Engineering effort.

4.8.2.5.1.1 Step 1: Identify RMA Program Objectives

This includes formulating RMA Program objectives under which the customer and vendor agree to participate in a structured RMA Engineering effort. Factors that should be considered for these objectives include:

- **Visibility** of progress and problems to the customer and vendor during the design effort
- **Controls** to ensure that adequate standards are being applied to the design, quality, and production of the system as related to RMA
- **Correction** to provide means to find and correct problems after the design effort
- **Communication** of information concerning the above factors within the vendor organization and to the customer
- **Demonstration** to show system compliance with RMA requirements

These requirements shall be allocated to the appropriate phases of the AMS cycle of the program. Appropriate FAA-approved reliability program standards (e.g., MIL-STDs and MIL-HDBKs) shall be followed in establishing objectives and requirements to ensure that a robust RMA Program will be instituted based on the five factors above.

4.8.2.5.1.2 Step 2: Structuring the RMA Program

Tasking for the RMA Program should be based on the following considerations:

- **AMS phase.** Will there be sufficient data available in the targeted phase to get full benefit from the RMA task?
- **System design.** Is the system design new, modified, or COTS? Generally, the more mature a system is, the less effort is required for RMA evaluation.
- **System complexity**. Generally, higher complexity requires more intensive RMA tasking.
- **Task utility.** Will the information provided by the task serve a constructive purpose? If the results will not be usable to correct system deficiencies, the task may not be cost effective to perform.
- **Cost.** Is the investment in the task worth the result?
- **Schedule impact.** Will the task affect the progress of the program or project?

- **Subcontractor control.** If subcontractors are involved, tasking must be considered to ensure that the prime vendor is qualifying subcontractor products for compliance with program requirements.

4.8.2.5.1.3 Step 3: Establish Performance-Monitoring Processes

Plans shall be developed early in the program to define processes to monitor RMA performance throughout the system lifecycle. It is recommended that an RMA data system be incorporated early in the system's lifecycle to support such monitoring and assessment of RMA performance, and to ensure that all recorded RMA data are appropriately disseminated, analyzed, and evaluated. Two relevant methodologies—FRACAS and the Reliability Growth Program—should be planned for most RMA programs and are described below.

4.8.2.5.1.3.1 FRACAS

In conjunction with an effective RMA data system, it is recommended that a closed-loop FRACAS be established to support problem detection, assessment, and correction. Such a system enables implementation and documentation of design improvements and corrections during the system development process. It also provides a tool for monitoring progress toward meeting system RMA requirements. The data collected supports tracking root causes of problems, which facilitates overcoming hurdles that may be hindering achievement of specific RMA requirements.

It is recommended that the FRACAS continue to be used during in-service operations to support upgrading of system RMA performance, in conjunction with a Reliability Growth Program (see next subsection), if necessary. Operational environments provide greater fidelity for demonstrating the actual capability of the system to meet RMA requirements.

4.8.2.5.1.3.2 Reliability Growth Program

Reliability growth, sometimes called Test Analyze And Fix (TAAF), is an ongoing process of testing to identify design, material, and specification deficiencies, as well as for performing corrective engineering changes. Failures that randomly occur due to normal wear and tear which are typically corrected by replacing parts are not within the scope of this effort. Statistical methods are used to predict the system MTBF at any point in time and to estimate the additional test time required to achieve a given MTBF goal.

To ensure a successful Reliability Growth Program, the contractor shall be aggressive in promptly correcting defects. One incentive for the contractor is the tradeoff between the Reliability Growth effort and the risk of passing Reliability Qualification tests for system acceptance. This is because it is better to discover defects during the TAAF effort, where they get corrected and credited for enhancing reliability growth, than to expose them during qualification testing, where they can hinder customer acceptance.

Another factor in implementing a Reliability Growth Program is its effect on the development schedule, taking into account the efforts involved in testing for and correcting defects. Other issues to be considered include:

- **COTS or newly developed systems.** TAAF benefits are limited for COTS items, since design changes are not within the purview of the customer.

- **State-of-the-art technology.** Systems based on cutting-edge technology would be expected to have more latent defects than more mature systems, incurring more resources.

- **System complexity.** More complex systems would be expected to have more latent defects, incurring more resources.

- **Number of target systems to be deployed.** More benefit from Reliability Growth efforts are realized as the number of fielded target systems increases. This should be taken into consideration when allocating resources to TAAF.

The success of a Reliability Growth effort depends on the following:

- Quality of test facilities

- Number of test systems allocated to the TAAF effort

- Scope and integration of the FRACAS into the Reliability Growth regimen

- Experience of the developer and availability of a priori data for similar systems

It is recommended that field personnel be involved in reliability growth testing and concur in deciding when the system is sufficiently stable to warrant deployment to the field.

4.8.2.5.1.4 Step 4: Report Results

Results of the performance-monitoring effort are reported to support assessment of the progress toward meeting requirements and meeting RMA program objectives. This includes comparing predicted and demonstrated RMA versus requirements and evaluating system RMA demand throughout the system’s operational life.

4.8.2.5.1.5 Step 5: Use Results for Planning, Managing, and Budgeting

Assessing progress toward meeting requirements and meeting RMA program objectives provides feedback to adjust program planning, management, and budgeting. The results may also be used to support related analyses, such as safety and logistics, and to emphasize improvements in succeeding systems.

4.8.2.5.2 Design Analysis Reports

There are various types of RMA analyses conducted and eventually documented within a Design Analysis Report. A discussion of some of the more common RMA-related analyses follows.

4.8.2.5.2.1 Failure Modes and Effects Analysis

FMEA is an evaluation process for analyzing and assessing the potential failures in a system. The objective is to determine the effect of failures on system operation, identify the failures critical to operational success and personnel safety, and assess each potential failure according to the effects on other portions of the system. In general, these objectives are accomplished by itemizing and evaluating system composition and functions.

FMEA is a systematic method of identifying the failure modes of a system, a constituent piece, or function and determining the effects on the next higher level of the design. The detection method (if any) for each failure mode may also be determined. An FMEA may be a quantitative or qualitative analysis and may be performed on all types of systems (e.g., electrical, electronic, or mechanical). If a quantitative FMEA is being performed, a failure rate is determined for each failure mode. The FMEA results may be used to support other analysis techniques, such as a fault tree analysis. Other techniques that are occasionally used include the dependence diagram and Markov analysis.

4.8.2.5.2.2 Failure Modes and Effects Criticality Analysis

FMECA identifies potential design weaknesses through a systematic analysis approach. It considers all possible ways in which a component may fail (the modes of failure); the possible causes for each failure; the likely frequency of occurrence; the criticality of failure; the effects of each failure on systems operation (and on various system components); and any corrective action that may be initiated to prevent (or reduce the probability of) the potential problem from occurring in the future.

Essentially, an FMECA is generated from an FMEA by adding a criticality figure of merit. More information on performing an FMECA appears in Section 9.7 of the FAA’s System Safety Handbook.

4.8.2.5.2.3 Fault Tree Analysis (FTA)

FTA is another approach to FMEA. It takes on a more general, functional view than the tabular FMEA, providing more visibility into the cause of a failure effect. Details on FTA contents and the steps involved in performing an FTA appear in Section 9.3 of the FAA’s System Safety Handbook.

4.8.2.5.3 Requirements

The following subsections provide general guidelines in developing candidate RMA requirements that may arise as a result of RMA Engineering analysis efforts.

4.8.2.5.3.1 RMA Requirements

For systems that are directly replacing existing systems, it is recommended that the RMA Engineering practitioner do the following:

- Locate the system being replaced within the higher level architecture
- Identify the service thread or threads that the system supports
- Determine the criticality level of the service thread; if more than one service thread is supported, use the service thread with the highest criticality level
- Use the availability associated with the service thread with the highest criticality level as the basis for the system-level availability requirement

For systems that are not replacing existing systems, it is recommended that the RMA Engineering practitioner do the following:

- Identify the criticality of the system according to the provided requirements
- Ensure that the requirements are consistent with the higher level requirements and the associated NAS Architecture implementation plan being addressed

The primary objectives in preparing the RMA provisions for a procurement package are to:

- Provide the specifications, including a system-level specification, defining the RMA requirements for the delivered system
- Define the effort required to provide the documentation, engineering, and testing to support monitoring of the design and development effort, risk management, design validation, and reliability-growth testing activities
- Provide guidance concerning the design and data required to facilitate technical evaluation of fault-tolerant design approaches, as well as programs for risk management, software fault avoidance, and reliability growth

The system-level specification serves as the basis for defining the design characteristics and performance that are expected of the system. From the standpoint of RMA characteristics, it is necessary to define the quantitative RMA and performance characteristics of the automatic fault detection and recovery mechanisms. It is also necessary to define the operational requirements needed to permit FAA facilities personnel to perform real-time monitoring and control and manual recovery operations as well as diagnostic and support activities.

4.8.2.6 RMA Tools

Tables 4.8.2-1 and 4.8.2-2 list the RMA tools.

Table 4.8.2-1. Reliability Analysis Tools and Techniques

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Alert Reporting	Document significant problem and nonconforming item data for exchange between the FAA and Government-Industry Data Exchange Program.	Identifies potential problems.	Used throughout a program (extends beyond just RMA).	As close to problem identification as possible.
Failure Mode and Effects (and Criticality) Analysis (FMEA/FMECA)	Perform a systematic analysis of the local and system effects of specific component failure modes; under FMECA, also evaluate the mission criticality of each failure mode.	Identifies potential single failure points requiring corrective action; identifies critical items and assesses system redundancy.	Recommended for consideration for all systems.	When a system block diagram is available; update throughout system design.

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Fault Tree Analysis (FTA)	Systematically identify all possible causes leading to system failure or an undesirable event or state.	Permits systematic, top-down, penetration to significant failure mechanisms.	Apply to critical (especially safety-critical) systems.	During system design.
Failure Reporting Analysis, Corrective Action System (FRACAS)	Provide a closed-loop system for documenting hardware and software anomalies, analyzing their impact on RMA, and tracking them to their resolution.	Ensures that problems are systematically evaluated, reported, and corrected.	All programs may benefit from some type of formal, closed-loop system.	Throughout system lifecycle.
Reliability Assurance Plan	Identify the activities essential in ensuring reliable performance, including design, production, and product operation.	Ensures that design risks are balanced against program constraints and objectives through a comprehensive effort calculated to contribute to system reliability over the mission lifecycle.	For all programs with reliability performance requirements.	During program planning.

Table 4.8.2-1. Reliability Analysis Tools and Techniques? Continued

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Reliability Modeling (Prediction/ Allocation)	Perform prediction, allocation, and modeling tasks to identify inherent reliability characteristics.	Aids in evaluating the reliability of competing designs.	Most hardware programs benefit where failure rates are needed for tradeoff studies, sparing analysis, etc.	Early in design.
Redundancy Switching Analysis	Perform a rigorous failure modes, effects, and criticality analysis (FMECA) at the part level for all interfacing circuits of redundant equipment.	Verifies that the failure of one of two redundant functions does not impair the ability to transfer to the second function.	Recommended for consideration for redundant equipment.	Early in design.
Reliability Tradeoff Studies	Compare all realistic alternative reliability design approaches against cost, risk, schedule, and performance impacts.	Aids in deriving the optimal set of reliability performance requirements, architecture, baselines, or designs.	Performed at some level on all systems; predictive techniques may be used.	Investment Analysis and Solution Implementation.
Reliability Growth Test Test, Analyze, and Fix (TAAF)	Conduct test and repair cycles to disclose deficiencies and demonstrate RMA improvement with permanent corrective action as a result of engineering changes.	Provides gradual evolution of a system to a state of higher reliability through design changes to correct design, part, or specification deficiencies.	Appropriate for all hardware and software systems.	Toward the end of design and throughout the product lifecycle.

Table 4.8-7. Reliability Analysis Tools and Techniques? Continued

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Environmental Stress Screening (ESS)	Apply mechanical, thermal, or other stresses to the target system to precipitate latent defects to failure.	Identify defects in parts, materials, and workmanship as manifested in the fabrication and production of the target system.	Complex systems, stressful deployment environment, low system maturity, high system packaging density, past experience with similar systems	Product phase.
Sneak Circuit Analysis	Methodically identify sneak conditions (unexpected paths or logic flows) in circuits.	Identifies design weaknesses that could inhibit desired functions or initiate undesired functions.	Generally used only for the most safety-critical equipment.	Early in design.
Trend Analysis	Evaluate variation in data with the ultimate objectives of forecasting future events based on examination of past results.	Provides a means of assessing the status of a program or the maturity of a system or equipment and predicting future performance.	Used to track failures, anomalies, quality processes, delivery dates, etc.	Throughout the program.

Table 4.8.2-2. Maintainability Analysis Tools

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Link Analysis	Arrange the physical layout of instrument panels, control panels, workstations, or work areas to meet specific objectives (e.g., increased accessibility).	Provides as assessment of the connection between (a) a person and a machine or part of a machine; (b) two persons; or (c) two parts of a machine.	During design for maintainability.	During Mission Analysis and Investment Analysis.
Maintainability Modeling (Prediction/ Allocation)	Perform prediction, allocation, and modeling tasks to estimate the system mean-time-to-restore requirements.	Determines the potential of a given design for meeting system maintainability performance requirements.	Whenever maintainability requirements are designated in the design specification.	Early in Solution Implementati on.
Maintenance Concept	Describe what, how, and where preventive and corrective maintenance is to be performed.	Establishes the overall approach to maintenance for meeting the operational requirements and the logistics and maintenance objectives.	Performed for any system where maintenance is a consideration.	During Mission Analysis and revised throughout the lifecycle.
Maintenance Engineering Analysis	Describe the planned general scheme for maintenance and support of an item in the operational environment.	Provides the basis for design, layout, and packaging of the system and its test equipment and establishes the scope of maintenance resources required to maintain the system.	A Maintenance Plan may be substituted on smaller programs in which maintainability prediction and analysis are not required.	Begins during design and iterated through development .

Table 4.8.2-2. Maintainability Analysis Tools—Continued

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Maintenance Plan	Detail how the support program is to be conducted to accomplish the program goals.	Identifies the desired long-term maintenance characteristics of the system and the steps for attaining them.	Appropriate for all hardware programs.	During Investment Analysis and update throughout the life of program.
Reliability Centered Maintenance (RCM)	Determine the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost.	Minimizes or eliminates more costly unscheduled maintenance and minimizes preventive maintenance.	Appropriate for all hardware programs; generally called for as part of the maintenance concept.	During Solution Implementation.
Testability Analysis	Assess the inherent fault detection and failure isolation characteristics of the equipment.	Improves maintainability in response to operational requirements for quicker response time and increased accuracy.	Applicable to all hardware systems; however, especially appropriate where maintenance resources are available but restrained.	Early in design.
Tradeoff Studies	Compare realistic alternative maintainability design approaches against cost, schedule, risk, and performance impacts.	Determines the preferred support system or maintenance approach in accordance with risk, performance, and readiness objectives.	Performed where alternate support approaches or maintenance concepts involve high-risk variables.	Complete early in the acquisition cycle (see Section 4.6).

4.8.2.7 RMA Metrics

At a minimum, RMA metrics are based on the system's MTBF (i.e., reliability), MTTR (i.e., maintainability), and availability. (See subsection 4.8.2.1.1 for further details.)

4.8.2.8 References

1. Guide to the Assessment of Reliability of Systems Containing Software. Document No. 89/97714. British Standards Institution, 12 September 1989.

2. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Aerospace Recommended Practice, ARP4761. Society of Automotive Engineers, Inc. Issued 1996-12.

3. *Reliability Engineer's Toolkit.* Rome Laboratory. Griffiss Air Force Base, April 1993.

4. *System Safety Handbook.* Federal Aviation Administration, 30 September 2000.

4.8.3 Human Factors Engineering

4.8.3.1 What Is Human Factors Engineering?

Human Factors Engineering (HFE) is a multifaceted discipline that generates information about human requirements and capabilities and applies it to the design and acquisition of complex systems (see Figure 4.8.3-1). HFE provides the opportunity to: (1) develop or improve all human interfaces with the system; (2) optimize human/product performance during system operation, maintenance, and support; and (3) make economical decisions on personnel resources, skills, training, and costs. Embedding and integrating HFE activities into the acquisition of systems and equipment lower lifecycle costs, improve overall performance, and reduce technical risk. Failure to apply the disciplines of HFE has consistently resulted in development of systems that do not satisfy the needs of the workforce and often results in costly delays and extensive rework.

Human Factors Engineering is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to:

- **Equipment, Systems, Software, Facilities**
- **Procedures, Jobs, Organizational Design, Environments**
- **Training, Staffing, Personnel management**

To produce safe, comfortable, and effective human performance.

Figure 4.8.3-1. Definition of Human Factors Engineering

4.8.3.2 Why Perform HFE?

Experience has proven that when people think of acquiring a system, they tend to focus on the hardware and the software. Individuals often fail to visualize the people who operate and maintain the hardware/software. The individuals and teams who operate or maintain the system have different aptitudes, abilities, and training, and they operate the hardware/software under various operating conditions, organizational structures, procedures, equipment configurations, and work scenarios. The total composite of these elements and the human component determines the performance, safety, and efficiency of the system in the National Airspace System. To produce an effective HFE program for any acquisition, one must not only define the system hardware, software, facility, and services, but also the *users* (operators and maintainers) and the *environment* in which the acquisition is used.

Applied early in the lifecycle acquisition management process, HFE enhances the probability of increased performance, safety, and productivity; decreases lifecycle staffing and training costs; and becomes well integrated into the program's strategy, planning, cost and schedule baselines, and technical tradeoffs. Changes in operational, maintenance, or design concepts during the later phases of an acquisition are expensive and entail high-risk program adjustments. Identifying lifecycle costs and human performance components of system operation and maintenance during investment analysis and requirements definition decreases program risks and long-term operations costs. These benefits apply to commercial-off-the-shelf (COTS) and non-developmental items (NDI) as well as to developmental programs.

4.8.3.3 Inputs to the HFE Process

The FAA Human Factors Job Aid guidelines are in the FAA Acquisition System Toolset (FAST). These guidelines contain extensive information regarding integration of HFE activities into the acquisition management process. It is recommended that product teams be familiar with this information and embed HFE principles into their acquisition programs. The Human Performance Interfaces in Systems Acquisition (Table 4.8.3-1) identify and define the many classes of human interfaces that the product team may need to consider as it plans and implements equipment/system acquisition programs. Analysis of these interfaces may provide a basis for determining the inputs to the HFE process tasks. These inputs may include new or previously conducted human factors research, studies, and analyses; human factors standards and guidelines; human factors technical methods and techniques; human performance data criteria; or other human-system interaction information.

Table 4.8.3-1. Human Performance Interfaces in Systems Acquisition

Human Interface Class	Performance Dimension	Performance Objective
Functional Role Interfaces: For operations and maintenance ? role of the human versus automation; functional requirements and tasks; manning levels; and skills and training	Task performance	Ability to perform tasks within time and accuracy constraints
Information Interfaces: Information media, electronic or hardcopy; information characteristics; and the information itself	Information handling/processing performance	Ability to identify, obtain, integrate, understand, interpret, apply, and disseminate information
Environmental Interfaces: Physical, psychological, and tactical environments	Performance under environmental stress	Ability to perform under adverse environmental stress, including heat and cold, vibration, clothing, illumination, reduced visibility, weather, constrained time, and psychological stress
Operational Interfaces: Procedures, job aids, embedded or organic training, and online help	Sustained performance	Ability to maintain performance over time

Table 4.8.3-1. Human Performance Interfaces in Systems Acquisition—Continued

Human Interface Class	Performance Dimension	Performance Objective
Organizational Interfaces: Job design, policies, lines of authority, management structure, organizational infrastructure	Job performance	Ability to perform jobs, tasks, and functions within the management and organizational structure
Cooperation Interfaces: Communications, inter-personal relations, and team performance	Team performance	Ability to collectively achieve mission objectives
Cognitive Interfaces: Cognitive aspects of human-computer interfaces (HCI), situational awareness, decisionmaking, information integration, and short-term memory	Cognitive performance	Ability to perform cognitive operations (e.g., solve problems, make decisions, integrate information, and have situational awareness)
Physical Interfaces: Physical aspects of the system with which the human interacts (e.g., HCI, controls and displays, workstations, and facilities)	Operations and maintenance performance	Ability to perform operations and maintenance at workstations and worksites, and in facilities using controls, displays, equipment, tools, and other instruments.

Addressing the human performance limitations and capabilities would seem to be a daunting task unless the task was divided into its many components and unless human factors is described in some descriptive taxonomy of issues. Thus, the potential human factors risks may be reflected as elements of the human factors areas of interest listed in Table 4.8.3-2.

Table 4.8.3-2. Human Factors Areas of Interest

Human Factors Areas of Interest
1. Allocation of Functional Roles: Assigning those roles/requirements/tasks for which the human or equipment performs better while enabling the human to maintain awareness of the operational situation.
2. Anthropometrics and Biomechanics: Accommodating the physical attributes of its user population (e.g., from the 1st through 99th percentile levels).
3. CHI (Computer-Human Interaction): Employing effective and consistent user dialogues, interfaces, and procedures across system functions.

Table 4.8.3-2. Human Factors Areas of Interest—Continued

Human Factors Areas of Interest
4. Communications and Teamwork: Applying system design considerations to enhance required user communications and teamwork
5. Culture: Addressing the organizational and sociological environment into which any change, including new technologies and procedures, will be introduced.
6. Displays and Controls: Designing and arranging displays and controls to be consistent with the operator's and maintainer's tasks and actions.
7. Documentation: Preparing user documentation and technical manuals in a suitable format of information presentation, at the appropriate reading level, and with the required degree of technical sophistication and clarity.
8. Environment: Accommodating environmental factors (including extremes) to which the system will be subjected and understanding the associated effects on human-system performance.
9. Functional Design: Applying human-centered design for usability and compatibility with operational and maintenance concepts.
10. Human Error: Examining design and contextual conditions (including supervisory and organizational influences) as causal factors contributing to human error, and considering objectives for error tolerance, error prevention, and error correction/recovery.
11. Information Presentation: Enhancing operator and maintainer performance by using effective and consistent labels, symbols, colors, terms, acronyms, abbreviations, formats, and data fields.
12. Information Requirements: Ensuring availability and usability of information needed by the operator and maintainer for a specific task when it is needed, and in a form that is directly usable.
13. I/O Devices: Selecting input and output (I/O) methods and devices that allow operators or maintainers to perform tasks, especially critical tasks, quickly and accurately.
14. KSAs: Measuring the knowledge, skills, and abilities (KSAs) required to perform job-related tasks, and determining appropriate selection requirements for users.
15. Operational Suitability: Ensuring that the system appropriately supports the user in performing intended functions while maintaining interoperability and consistency with other system elements or support systems.
16. Procedures: Designing operation and maintenance procedures for simplicity, consistency, and ease of use.
17. Safety and Health: Preventing/reducing operator and maintainer exposure to safety and health hazards.
18. Situational Awareness: Enabling operators or maintainers to perceive and understand elements of the current situation, and project them to future operational situations.
19. Special Skills and Tools: Minimizing the need for special or unique operator or maintainer skills, abilities, tools, or characteristics.
20. Staffing: Accommodating constraints and efficiencies for staffing levels and organizational structures.

Table 4.8.3-2. Human Factors Areas of Interest—Continued

Human Factors Areas of Interest
21. Training: Applying methods to enhance operator or maintainer acquisition of the knowledge and skills needed to interface with the system, and designing that system so that these skills are easily learned and retained.
22. Visual/Auditory Alerts: Designing visual and auditory alerts (including error messages) to invoke the necessary operator and maintainer response.
23. Workload: Assessing the net demands or impacts upon the physical, cognitive, and decisionmaking resources of an operator or maintainer using objective and subjective performance measures.
24. Work Space: Designing adequate work space for personnel and their tools or equipment, and providing sufficient space for the movements and actions that personnel perform during operational and maintenance tasks under normal, adverse, and emergency conditions.

4.8.3.4 HFE Process

The process of integrating HFE into acquisition programs entails numerous technical and management activities. Many of these activities are conducted iteratively through several phases of the acquisition and often in a nonlinear sequence. While the process flow is described in the 14 activities listed in Table 4.8.3-3, other subordinate activities (e.g., critical task analysis, target audience analysis, cognitive analysis, human-in-the-loop simulation, and HCI prototyping) are also required. A description of these subordinate tasks is in the FAA Human Factors Job Aid or in more detailed HFE reference manuals.

Table 4.8.3-3. HFE Process Activities

HFE Process Activities
1. Incorporate Human Factors Opportunities and Constraints Into the Mission Analysis and Service Level Mission Need 2. Incorporate Human Factors Requirements in Program Requirements 3. Incorporate Human Factors Assessment in the Investment and Business Case Analysis 4. Incorporate Human Factors Parameters in Program Baselines 5. Designate Human Factors Coordinator for the Service Organization(s) 6. Establish Human Factors Working Group 7. Incorporate Human Factors Strategy and Tasks into the Program Implementation Strategy and Planning 8. Develop Integrated Human Factors Plan 9. Incorporate Human Factors Requirements into System Specifications and Statements of Work 10. Include Human Factors in Source Evaluation Criteria 11. Conduct HFE Analyses 12. Apply HFE to System Design 13. Test System Against Human Performance Requirements 14. Incorporate Human Factors Considerations in Post-Implementation Review

4.8.3.5 HFE Process Tasks

The following process flow provides an outline and overview of key activities in the HFE process.

Activity 1: Incorporate Human Factors Opportunities and Constraints Into the Mission Analysis (MA) and Service Level Mission Need (SLMN)		
Product	**Approval Authority**	**Tools and Aids**
Human factors input on opportunities and constraints to the SLMN	Mission analysis manager SLMN sponsor	Human Factors Acquisition Job Aid (Chapter 4) guidance on developing human factors input to the MA and SLMN "Human Factors Integration Guide for Mission and Service Area Analysis"

Description:

Using the results from the MA, HFE inputs to the SLMN identify the human performance constraints and issues that need to be addressed or resolved. This information may come from operations and maintenance analyses or concepts and other documents that may provide insights into the effects of HFE constraints and limitations on mission and system performance. Since most acquisitions are evolutionary, important HFE information may be obtained from predecessor architectures, systems, or their component subsystems. Analyses and tradeoff studies may be required to determine the effects of constraints and issues on system performance. It is recommended that the existing literature and lessons learned databases be reviewed.

Activity 2: Incorporate Human Factors Requirements in Program Requirements		
Product	**Approval Authority**	**Tools and Aids**
Human factors requirements in the preliminary and final program requirements documents	Requirements development lead	Human Factors Acquisition Job Aid (Chapter 4) guidance on developing human factors requirements for requirements documents "Guidelines for Human Factors Requirements Development"

Description:

The preliminary and final program requirements documents contain performance and supportability requirements that do not prescribe a specific solution. The requirements document defines the essential performance capabilities and characteristics, including those of the human component. HFE inputs to the requirements document identify human performance factors that impact system design. Cognitive, physical, and sensory requirements are established for the operator, maintainer, and support personnel that contribute to or constrain total system performance. It is recommended that any safety, health hazards, or critical errors that reduce job performance or system effectiveness be defined, and that staffing and training concepts—including requirements for training devices, embedded training, and training logistics—also be described.

Activity 3: Incorporate Human Factors Assessment in the Investment and Business Case Analysis		
Product	**Approval Authority**	**Tools and Aids**
Human factors input to the investment and business case analysis plan Human Factors Assessment (including risk, cost, and benefits)	Investment and business case analysis lead	Human Factors Acquisition Job Aid (Chapter 5) guidance on developing Human Factors Assessments for the investment and business case analysis "Human Factors Assessments in Investment Analysis: Definition and Process Summary for Cost, Risk, and Benefit"

Description:

For each alternative being evaluated, HFE inputs to the investment and business case analysis address the full range of human performance and interfaces (e.g., cognitive, organizational, physical, functional, and environmental) to achieve an acceptable level of performance for operating, maintaining, and supporting the system. It is recommended that the analysis provide information on what is known and unknown about human performance risks in meeting minimum system performance requirements. HFE areas of interest relevant to the investment and business case analysis include:

- Human performance (e.g., human capabilities and limitations, workload, function allocation, hardware and software design, decision aids, environmental constraints, team versus individual performance)
- Training (e.g., length of training, training effectiveness, retraining, training devices and facilities, embedded training)
- Staffing (e.g., staffing levels, team composition, organizational structure)
- Personnel selection (e.g., aptitudes, minimum skill levels, special skills, experience levels)
- Safety and health hazards (e.g., hazardous materials or conditions, system or equipment safety design, operational or procedural constraints, biomedical influences, protective equipment, required warnings and alarms)

Activity 4: Incorporate Human Factors Parameters in Program Baselines		
Product	**Approval Authority**	**Tools and Aids**
Human factors performance parameters in the program baselines	Business case analysis lead	Human Factors Acquisition Job Aid (Chapter 4) guidance on developing human factors parameters for acquisition program baselines (Exhibit 300 Attachment 1) and the business case analysis (Exhibit 300 Attachment 2) "Guidelines for Human Factors Requirements Development"

Description:

The program baselines established at the Investment Decision reflect the solution selected by the acquisition authority for implementation. Based on this solution, HFE inputs to the acquisition program baselines are those human performance requirements needed to achieve the required level of system performance. These inputs are derived from the specified system performance levels identified in program requirements documents (preliminary Program Requirements and final Program Requirements). They reflect a progressive refinement that provides increased definition, greater granularity, and more specificity of relevant human-system performance characteristics. It is recommended that constraints, limitations, and unique or specialized training requirements, staffing levels, or personnel skill requirements be identified.

It is also recommended that, to the degree possible, the required level of human performance be based on practical measures of operational effectiveness and suitability and be stated in quantifiable terms (e.g., time to complete a given task, level of accuracy required, and number of tracks to be processed per unit time).

Activity 5: Designate Human Factors Coordinator for the Service Organization(s)		
Product	**Approval Authority**	**Tools and Aids**
Human Factors Coordinator	System engineer	Human Factors Acquisition Job Aid (Chapter 3) guidance on developing a human factors program

Description:

The Service Organization designates a Human Factors Coordinator to develop, direct, and monitor HFE activities during system acquisition. It is recommended that this designation occur as early as possible during investment and business case analysis to ensure that human considerations are an integral element of market surveys, tradeoff analyses, and the definition of requirements for candidate solutions to mission need. The Human Factors Coordinator:

- Defines human impacts and constraints during investment analysis and determines of requirements
- Evaluates human-system interfaces during market surveys, tradeoff analyses, and prototypes
- Prepares and updates HFE portions of program planning documents, procurement packages, performance criteria and measures, and data collection efforts
- Develops and analyzes operational scenarios and human-system modeling for operators and maintainers
- Reviews and assesses HFE concepts and designs
- Coordinates HFE efforts and workgroup activities
- Coordinates HFE with other disciplines

Activity 6: Establish Human Factors Working Group		
Product	**Approval Authority**	**Tools and Aids**
Human Factors Working Group Charter	System engineer	Human Factors Acquisition Job Aid (Chapter 3) guidance on human factors working groups

Description:

The Human Factors Coordinator may establish and chair a Human Factors Working Group (HFWG) to facilitate accomplishment of HFE tasks and activities. The composition of the HFWG is tailored to the needs of the acquisition program. Membership typically consists of Service Organization members, with outside members participating as needed.

Activity 7: Incorporate Human Factors Strategy and Tasks Into the Program Implementation Strategy and Planning		
Product	**Approval Authority**	**Tools and Aids**
Human factors strategy and tasks in the program Implementation Strategy and Planning document	System Engineer	Human Factors Acquisition Job Aid (Chapter 3) guidance for developing human factors strategy and tasks for the acquisition program

Description:

The human factors strategy depends on the size, cost, and complexity of the system to be acquired, as well as the nature and complexity of the human-product interface. It is recommended that the HFE strategy address such factors as:

- Scope and level of HFE
- HFE roles and responsibilities of organizations and contractors
- Means for evaluating the human-machine interface and achieving user buy-in
- Data sources and facilities needed
- Distribution of funding and resources
- Timing and scope of HFE activities
- Relationship of HFE with other program elements.

The HFWG may assist in developing strategies appropriate for different types of acquisition programs, such as those that procure NDIs, COTS products, or fully developed new systems.

The human factors tasks and activities define the HFE work to be done during program implementation. For each task, the program planning documentation assigns the responsible person and organization, identifies any output and the approval authority, specifies when the task is to be completed, and allocates resources. As the program progresses through Solution Implementation, the human factors portion of the program plan is updated to reflect changes in program strategy or execution and to provide more planning detail as it is developed.

Activity 8: Develop Integrated Human Factors Planning Information		
Product	**Approval Authority**	**Tools and Aids**
Integrated Human Factors Plan	Service Organization lead	Human Factors Acquisition Job Aid (Chapter 3) template for Integrated Human Factors Plan

Description:

For well-managed system acquisition programs, the Service Organization prepares an Integrated Human Factors input to the System Engineering Management Plan. (See Table 4.8.3-4 for an outline of the content.) Tasks associated with this plan include:

- Defining the operational concept and support concept
- Describing the target population
- Defining human/system interfaces
- Defining human impacts of the system
- Defining the HFE strategy
- Defining HFE implementation tasks and activities

Activity 9: Incorporate Human Factors Requirements Into System Specifications and Statements of Work

Product	Approval Authority	Tools and Aids
Human factors requirements in the System Specification Human Factors tasks in the Statement of Work Human Factors data items in the Contractor Deliverable Requirements List (CDRL) Human Factors data item descriptions	Service Organization lead	Human Factors Acquisition Job Aid (Chapter 6) guidance on formulating human factors requirements in the System Specification Human Factors Acquisition Job Aid (Chapter 7) guidance on defining human factors tasks in the Statement of Work Data Item Descriptions (FAA-HF-001 through FAA-HF-005) for human factors

Description:

The System Specification and Statement of Work translate human performance requirements and appropriate HFE work tasks to the contractor in a clear, unambiguous, and contractually binding document. The System Specification addresses the following elements to ensure that required human performance effectively influences system design:

- Staffing constraints
- Required operator and maintainer skills
- Training time and cost for formal, informal, and on-the-job skill development
- Acceptable levels of human and system performance when operated and maintained by the training population

The Statement of Work shall contain all human factors tasking to be imposed on the contractor, as well as define data deliverables in the CDRL and associated Data Item Descriptions (DID).

Activity 10: Include Human Factors in Source Evaluation Criteria		
Product	**Approval Authority**	**Tools and Aids**
Human factors source evaluation criteria	Service Organization lead	Human Factors Acquisition Job Aid (Chapter 8) guidance for specifying human factors in source selection

Description:

It is recommended that human performance be a candidate as a major evaluation factor in source selection. By providing vendors a clear indication that the government attributes significant weight to how operators and maintainers perform with the system, the agency sends a strong message that operational suitability and effectiveness are of utmost importance.

Activity 11: Conduct HFE Analyses		
Product	**Approval Authority**	**Tools and Aids**
Appropriate government or contract analyses and data such as those specified in the CDRL and DIDs	Appropriate government or contract official as designated in the CDRL (or other designated documentation)	Human Factors Acquisition Job Aid (Chapter 9) guidance for integrating human factors in system engineering Human Factors Design Standard, HF-STD-001 Human Factors Data Item Descriptions FAA-HF-001 through FAA-HF-005

Description:

The responsible Service Organization oversees, monitors, and reviews HFE analyses conducted by the implementation organization. These analyses may involve:

- Defining and allocating system requirements (e.g., human factors requirements analysis, staffing analysis, training analysis)
- Analyzing information flow and processing (e.g., information requirement analysis, CHI design analysis)
- Estimating operator and maintainer capabilities (e.g., task performance analysis, training performance analysis, time and motion study, safety analysis)
- Defining and analyzing physical and cognitive tasks and workloads (e.g., task analysis, job design analysis, organizational design analysis)
- Identifying and measuring human error risks and defining their mitigation and impact on design, equipment, procedures, and task performance (e.g., human reliability analysis for Reliability, Maintainability, and Availability Engineering; human factors safety analysis; and human factors risk assessment)

Activity 12: Apply HFE to System Design		
Product	**Approval Authority**	**Tools and Aids**
Implementation of Human Engineering Program Plan Integration of Human factors requirements into system design	System engineer	Human Factors Acquisition Job Aid (Chapter 9) guidance for integrating human factors in system engineering Human Factors Design Standard, HF-STD-001

Description:

HFE is applied to system design activities to optimize human-system interfaces and ensure that human performance requirements are satisfied. HFE is applied to the full scope of system design, including experiments, tests, and studies; engineering drawings; work environment, crew station, and facility design; performance and design specifications; procedure development; software development; and manuals. The following are used effectively in defining human-product interfaces during system design:

- Prototypes and computer models
- Three-dimensional mockups
- Scale models
- Dynamic simulation

Activity 13: Test System Against Human Performance Requirements		
Product	**Approval Authority**	**Tools and Aids**
Test results on human performance requirements	System engineer System test official	Human Factors Acquisition Job Aid (Chapter 10) guidance on HFE activities during test and evaluation

Description:

Testing to see if the system complies with human performance requirements is performed as early as possible in system development. HFE findings from design reviews, prototype reviews, mockup inspections, demonstrations, and other early engineering tests are used in planning and conducting later tests. HFE testing focuses on verifying that user personnel in the intended operational environment are able to operate, maintain, support, and control the system.

Activity 14: Incorporate Human Factors Considerations in Post-Implementation Review		
Product	**Approval Authority**	**Tools and Aids**
Assessment of the acceptability of the human-system interface and performance Post-Deployment Human Factors Assessment Plan	System engineer	Human Factors Guidance on Conducting Human Factors Post-Implementation Reviews FAA policy and guidance on Post-Implementation Reviews In-Service Management Review Checklist (Section 6)

Description

Operational suitability and effectiveness are major evaluation factors that are considered in making the decision to place a new capability into operational service. Satisfactory human performance is an integral element of operational suitability and effectiveness. The broad range of HFE issues is addressed during this activity. Also, a plan is formulated to assess and monitor the human-system performance of the new capability following its deployment to the operational environment.

4.8.3.6 HFE Process Outputs/Products

Efforts to manage the HFE program, establish requirements, conduct system integration, and test and evaluate HFE compliance may result in many major and minor HFE outputs and products. These products include human factors input to the primary acquisition documentation as well as human factors research, studies, and analyses that support program and design decisions and documentation (e.g., human factors risk analyses, human factors benefits analyses, criteria for performance evaluation, prototype designs, and critical task analyses). The HFE activities and their resultant products are described in more detail in the FAA Human Factors Job Aid (and other HFE manuals), but are reflected in the following five key components of program planning and implementation.

4.8.3.6.1 HFE Planning Criteria

HFE planning involves developing concepts, tasks, completion dates, levels of effort, methods to be used, strategy for development and verification, and an approach to implementing and integrating with other program planning. This information is sent to Integrated Technical Planning (Section 4.2).

4.8.3.6.2 HFE Analysis Reports

HFE analysis involves identifying the best allocation of roles/tasks/requirements to personnel, equipment, software, or combinations to meet the acquisition objectives. It includes dissecting functions to specific tasks, analyzing tasks to determine human performance parameters, quantifying task parameters to permit evaluation of human-system interfaces in relation to total system operation, and identifying high-risk HFE areas.

4.8.3.6.3 HFE Design and Development Analysis Reports

HFE design and development involves converting mission, system, and task analyses data into (1) detail designs and (2) development plans to create human-system interfaces that operate within human performance capabilities, meets system functional requirements, and accomplishes mission objectives. (See Trade Studies (Section 4.6).)

4.8.3.6.4 HFE Test and Evaluation Analysis Reports

HFE test and evaluation involves verifying that systems, equipment, software, and facilities may be operated and maintained within intended user performance capabilities and is compatible with overall system requirements and resource constraints. (See Validation and Verification (Section 4.12).)

4.8.3.6.5 HFE Management and Coordination Analysis Reports

HFE management and coordination involves coordinating with and providing input to reliability, maintainability, and availability engineering; system safety; risk management; facilities and systems engineering; integrated logistic support; and other HFE functions, including biomedical, personnel, and training functions.

4.8.3.7 References

1. Boff, K., and Lincoln J., eds. *Engineering Data Compendium: Human Perception and Performance.* Vols. *1- 3.* Wright-Patterson Air Force Base, OH: Harry G. Armstrong Aerospace Medical Research Laboratory, 1988.

2. Booher, H. R., ed. *Handbook of Human Systems Integration*, New York, NY: John Wiley & Sons, 2003.

3. Booher, H. R., ed. *MANPRINT: An Approach to Systems Integration*, New York, NY: Van Nostrand Reinhold, 1990.

4. Cardosi, K. M., and Murphy, E. D., eds. *Human Factors in the Design and Evaluation of ATC Systems.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, April 1995.

5. *Definitions of Human Factors Terms*. MIL-HDBK-1908, August 1999.

6. *FAA Human Factors Design Standard.* Document HF-STD-001. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2003. (http://hf.tc.faa.gov/hfds/)

7. *Human Engineering Design Guidelines*. MIL-HDBK-759C, July 1995.

8. *Human Engineering Program Process and Procedures*. MIL-HDBK-46855A, May 1999.

9. *Human Factors Job Aid Guidelines*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 2003. (http://fast.faa.gov/archive/v0200/human/htm/ccontent.htm)

10. *Human Factors Policy.* FAA Order 9550.8. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 2005.

11. Meister, D. *Behavioral Analysis and Measurement Methods*. New York, NY: John Wiley & Sons, 1985.

12. National Research Council. *Flight to the Future: Human Factors in Air Traffic Control*. Washington, DC: National Academy Press, 1997.

13. National Research Council. *The Future of Air Traffic Control: Human Operators and Automation.* Washington, DC: National Academy Press, 1997.
14. Salvendy, G., ed. *Handbook of Human Factors and Ergonomics.* 2nd edition New York, NY: Wiley-Interscience, 1997.
15. Sanders, M. S., and McCormick, E. J. *Human Factors in Engineering and Design.* 7th edition. New York, NY: McGraw-Hill, 1993.
16. *The National Plan for Civil Aviation Human Factors.* Washington, DC: U.S. Department pf Transportation, Federal Aviation Administration, 1995.
17. Wickens, C. D. *Engineering Psychology and Human Performance.* 2nd edition, New York, NY: Harper Collins, 1992.
18. Wiener, E. L., and Nagel, D. C., eds. *Human Factors in Aviation*. New York: Academic Press, 1998.

4.8.4 Electromagnetic Environmental Effects and Spectrum Management

Electromagnetic Environmental Effects (E^3) and Spectrum Management are two closely related areas of Specialty Engineering. They differ, however, in several ways, and the following sections discuss each area separately, starting with E^3.

4.8.4.1 Electromagnetic Environmental Effects

E^3 Engineering is the technical discipline dealing with safe and efficient operation of electronic devices regarding radiated and conducted electromagnetic emissions. This includes both a given system's ability to deal with such emissions from its operational environment and how the device itself affects that environment. E^3 activities seek to minimize a system’s limitations that are due to electromagnetic factors, as well as document limitations and vulnerabilities that remain after a system's deployment.

4.8.4.1.1 What Is Electromagnetic Environmental Effects Engineering?

E^3 Engineering is a set of Specialty Engineering analyses/requirements that relate to electronic systems. Such systems range from electric household appliances to integrated circuits.

The Federal Communications Commission (FCC) develops and enforces government regulations related to E^3 and gives special attention to what it calls "digital devices." The FCC defines a digital device as:

> *Any unintentional radiator (device or system) that generates and uses timing pulses at a rate in excess of 9000 pulses (cycles) per second and uses digital techniques . . .*

In other words, digital devices are any electronic devices using high-speed switching waveforms. These devices usually generate significant electromagnetic interference (EMI) and shall be designed to conform to government regulations on electromagnetic emissions.

All systems deployed in the NAS shall conform to government regulations. E^3 analyses shall be performed to ensure that all electronic systems function properly within an operational environment and that they are compatible with nonelectronic elements of that environment. These analyses shall also identify problems that could arise from changes in the environment.

There are many types of E^3 that may affect a system’s electromagnetic compatibility. Each type is an individual specialty area. From a broad perspective, the operational requirements are to properly address the electromagnetic environment over the system lifecycle. The following sections discuss the individual elements of E^3. (Note: E^3-related definitions appear in American National Standards Institute (ANSI) C63.14.)

4.8.4.1.1.1 The Electromagnetic Environment

The Electromagnetic Environment (EME) consists of the systems and other elements (i.e., humans and nature) that exist within the area where a given system is or may be operated. Identifying and describing the EME is a major part of E^3. This involves describing all EMI within the environment and vulnerabilities to systems and other elements of the environment.

It is important to develop a complete description of the normal EME within which the system, subsystem, or equipment may be required to perform. In some instances, commercial-off-the shelf (COTS) systems have defined the *survivable* EME for a system; that is, the most extreme conditions (EMI present) within which the system may operate safely and without degrading its function.

4.8.4.1.1.2 Electromagnetic Compatibility

A key area of E^3 is Electromagnetic Compatibility (EMC). This is the ability of a system to function within its EME and not be a source of troublesome EMI. EMC analyses involve evaluating the EME (all EMI present within that environment) and the new system's own EMI emissions. This data is then used to determine if either the new system or the elements of the operational environment adversely affect each other. EMC considerations are critically important and must be seen as design objectives beyond those required for the basic functional performance of an electronic system. This ensures that a system that functions properly in the laboratory will not have problems when it is deployed within a different EME. Invoking FAA-G-2100, paragraph 3.3.2 Electromagnetic Compatibility—a requirement for any acquisition, which references all appropriate FCC rules and FAA-referenced Military Standards—ensures consideration of EMC throughout the system lifecycle.

Two general types of emissions are considered in an EMC analysis that evaluates EMI: conducted emissions and radiated emissions. Conducted emissions are electric currents transferred through physical coupling, such as noise fed back into a device's alternating current (AC) power system. Radiated emissions are EM waves emitted intentionally or unintentionally that may be unintentionally received by other systems. Wires transmit and receive EM signals like intentional antennas. Switching waveforms in circuits generate a wide band of EM emissions.

4.8.4.1.1.3 Electromagnetic Susceptibility

EM Susceptibility (EMS) specifically deals with a system's weaknesses or lack of resiliency regarding certain EM conditions. A *susceptibility* is a condition that causes a system to be degraded. For example, conducted susceptibility refers to a system's inability to withstand an infusion of noise into its power lines. Devices that run on standard AC power shall not be susceptible to sudden brief spikes or losses of power if the power system is affected by lightning or other surges.

A system may be exposed to different operational EMEs during its lifetime. A system that degrades within certain potential EMEs is said to be *vulnerable*. A vulnerability analysis shall be conducted to determine the operational impacts of laboratory-observed susceptibilities.

4.8.4.1.1.4 Hazards of Electromagnetic Radiation

Hazards of EM Radiation (RADHAZ) are areas of E^3 that deal with specific types of dangers related to radiated EM waves. The two primary RADHAZ evaluated are Hazards of EM Radiation to Fuels (HERF) and Hazards of EM Radiation to Personnel (HERP). HERF is a RADHAZ area dealing with fuels that may be present within an EME. An EM field of sufficient intensity may create sparks that may ignite volatile combustibles, such as fuel. (i.e., EM radiation may induce a current in a conductive material, and sparks are formed in the air gap between two conductors.) It is difficult to locate all potential antennas and spark gaps within an EME, so it is necessary to keep the power densities of EM fields within safety margins when fuels are present.

HERP deals with the dangers of radiation to humans within the EME. When a person absorbs microwaves, the body heats up. Microwave absorption at high power levels (i.e., from radar towers) is sometimes hazardous. Also, EM waves in the x-ray range and higher (in terms of frequency) may cause ionization, even at low power levels. Considering RADHAZ in the E^3 analysis ensures safety for the nonelectronic elements of an EME.

4.8.4.1.1.5 Electromagnetic Pulse

An EM Pulse (EMP) is an intense burst of EMI caused by a nuclear explosion. This pulse may damage sensitive electronic systems or cause them to temporarily malfunction. Evaluating the need to perform an analysis on EMP susceptibility is recommended.

4.8.4.1.1.6 Electrostatic Discharge

An Electrostatic Discharge (ESD) is an unintentional transfer of static electricity from one object to another. Static voltage transferred from a human to a device (e.g., voltage generated by walking across a carpet) may be as high as 25 kilovolts. The brief currents created may damage or cause malfunction of integrated circuits and other electronics. Evaluating the need to perform an ESD susceptibility analysis is recommended.

4.8.4.1.1.7 Lightning

Lightning gets special attention within E^3 because of its tremendous power levels and multiple effects. Lightning effects are *direct* (physical effects) and *indirect* (induced electrical transients and interaction of the EM fields associated with lightning). Determining a need for analysis for susceptibility to lightning is recommended.

4.8.4.1.1.8 Precipitation Static

Precipitation Static (P-Static) is the buildup of static electricity resulting from an object's exposure to moving air, fluid, or tiny solid particles (e.g., snow or ice). It may cause significant ESD and is a particularly important consideration regarding systems aboard aircraft and spacecraft. Evaluating the need for an analysis on P-Static susceptibility is recommended.

4.8.4.1.2 Why Perform E^3 Activities?

The following subsections discuss the key reasons for incorporating E^3 activities into the SE process.

4.8.4.1.2.1 Government Regulations

The FCC develops and enforces government regulations relating to E^3. Before a new electronic device may be sold in the United States, it shall meet the FCC's standards. These standards are in Rules and Regulations of Title 47 (Part 15) of the Code of Federal Regulations.

FCC requirements focus on a system's generated EMI, rather than its EMS. The requirements impose limits on the conducted and radiated emissions of digital devices and strictly regulate radiated emissions in terms of the electric field. Most NAS-related electronic/radio frequency devices fall under FCC Class A (commercial, industrial, or business). Regulations are less stringent for Class A than for Class B (household) devices. Government regulations change frequently, so it is important to obtain the most current requirements. Information is available from the FCC Web site (www.fcc.gov). The FCC may request a sample device of a new system to test.

4.8.4.1.2.2 System Performance and Cost of Redesign

While manufacturers and developers strive to meet government regulations, they may impose additional E^3 requirements on a new system to enhance product performance and customer satisfaction. Government E^3 requirements do not guarantee a new system's compatibility with its intended operational environment. Thus, it is up to manufacturers and developers to consider the EME for a new system, the impacts of the system's own EMI on that environment, and the system's EMS in order to avoid potential problems that FCC regulations are unable to predict or prevent.

Developers and manufacturers who consider potential E^3 problems from the start may avoid costly redesign later. The earlier in a system's lifecycle that a problem is identified, the less the cost of correcting it is likely to be. For instance, if a problem with EMC is discovered after a new system has been deployed, the system may have to undergo extensive redevelopment. However, if this problem had been determined during the design and planning stage, it could have been addressed in the requirements before manufacture had begun, saving both significant time and resources.

4.8.4.1.2.3 Hazard Prevention

Hazards of EM radiation on fuels and personnel (HERF, HERP) are important considerations. These issues may be included as part of Safety Risk Management activities.

4.8.4.1.2.4 International Considerations

EMI is increasing throughout the world. Systems that may be used outside of the United States, such as avionics, shall be able to deal with types and intensities of EMI present in other countries that may be different from conditions in the United States. It is recommended that such systems be designed specifically focusing on minimizing vulnerability to EM radiation. Also, it is recommended that consideration be given to the possibility of intentional jamming, which creates significant EMI.

4.8.4.1.3 Analyses of Electromagnetic Environmental Effects

While Section 4.8.0.3 describes the Specialty Engineering process in general terms, this section specifically discusses the various E^3- related analyses. Not all E^3 analyses discussed, however, are necessary for a given system. It is recommended that it be determined during planning which analyses are worth the time and resources.

It is recommended that E^3 analyses be performed on COTS systems as well as new systems to ensure compatibility with the EME within which these systems or subsystems may be used. The amount of detail involved with E^3 analyses increases with each subsequent phase of the SE lifecycle. Measurement procedures for evaluating a product's emissions during low-level technical analyses shall be clearly spelled out. It shall be understood how the results are to be interpreted. The EME may undergo appreciable changes at any point during a system's lifecycle. Thus, E^3 analyses shall be reconducted to ensure continued EMC of *each* system within the EME.

4.8.4.1.3.1 Description of the Operational Electromagnetic Environment

Before any EMC analyses are conducted, it is necessary to describe the EME within which the system in question may perform. This means detailing all sources of EMI in the operational environment. EME contributors are gauged by the power levels and frequencies of their emissions and their locations (with respect to the new system). In some cases, it may also be advisable to denote inherent susceptibilities associated with other systems within the EME.

An existing OSED document may be useful as a starting point for an EME description.

The OSED contains information about the operational environment and the systems/subsystems associated with the system under analysis. However, the OSED may not describe all EME contributors.

Optionally, a description may be developed of the maximum survivable EME conditions in which the system shall be able to function without degradation. This is useful in cases in which a specific operational EME may not be identified (e.g., the system may have numerous and appreciably different operational EMEs to which it is expected to be exposed).

4.8.4.1.3.2 Electromagnetic Compatibility Analyses

EMC analyses identify compatibility issues relating to radiated and/or conducted emissions. This involves evaluating how the EME and the system affect each other in terms of EMI.

It is useful to calculate the system's *electrical dimensions* before an EMC analysis is conducted. This is done to determine whether or not simple mathematical methods (e.g., Kirkchoff's Laws) are sufficiently accurate for an EMC analysis. If the system is *electrically large*, then simple mathematics is insufficient, and Maxwell's Equations shall be employed. These are a set of differential equations that describe an electric field as three-dimensional parameters (x, y, z) and time (t).

4.8.4.1.3.2.1 Federal Communications Commission Regulations

It is convenient to address FCC compliance issues for EM emissions during EMC analyses since both deal with the system's EMI. While actual testing to verify that FCC requirements are met may not occur until a system is built, incorporating these regulations into requirements from the beginning of system development helps to mitigate compliance problems later.

4.8.4.1.3.3 Analyses of Hazards of Electromagnetic Radiation

RADHAZ analyses are conducted only when they have relevance for a particular system and its environment. For example, if there are no fuels present within the operational EME, an HERF analysis is unnecessary. It is recommended that the types of RADHAZ analyses (if any) to be performed be determined from the EME description.

4.8.4.1.3.4 Electromagnetic Susceptibility Analyses

As with RADHAZ, specific susceptibility analyses are conducted only when they have relevance. Each analysis requires time and resources, so it is impractical to invest in an analysis that has no significance for the system and its EME. Susceptibility analyses include:

- Conducted Susceptibility (AC power lines)

- ESD Susceptibility
- Susceptibility to Lightning
- P-Static Susceptibility
- EMP Survivability

4.8.4.1.4 Outputs and Products of Electromagnetic Environmental Effects

It is important to employ E^3 analyses and predictions during all phases of an electronic system's lifecycle. Figure 4.8-1 (at the beginning of Section 4.8) illustrates the fundamental Specialty Engineering process and its outputs. The following sections link the outputs of E^3 activities to the overall SE process. However, note that all E^3 analyses, like other Specialty Engineering analyses, shall be documented in a Design Analysis Report.

4.8.4.1.4.1 Requirements

Most E^3 activities result in requirements that feed the Requirements Management process (Section 4.3). This includes the Mission Need Statement, Statement of Work, specifications, and all performance-based requirements.

4.8.4.1.4.2 Concerns and Issues

It is recommended that E^3 activities—in addition to identifying necessary requirements—also identify potential problems that may surface later in a system's lifecycle. It is also good practice to document identified system susceptibilities that are not significant enough to require correction. These issues are included with concerns and issues, which feed the Risk Management process (Section 4.10).

4.8.4.1.4.3 Verification Criteria

It is critical to provide verification criteria to ensure that stated E^3 performance requirements are met. It is also important to provide detailed information describing how E^3 testing is performed and how test results are to be interpreted. This feeds the Validation and Verification process (Section 4.12).

4.8.4.1.4.4 Solutions to Problems of Electromagnetic Environmental Effects

EMC and EMS problems may be corrected through a number of means, including shielding, emission suppression components, and/or modification of the operational environment. However, some problems may not be directly correctable, potentially forcing extensive and costly product redesign. This is why it is beneficial to consider E^3 issues early in a system's development.

4.8.4.2 Spectrum Management

The radio frequency (RF) spectrum is that portion of the EM spectrum used for *deliberately* transmitting and receiving signals. It is a finite set of frequencies that must be divided efficiently between various government and civilian industries. The FAA, Air Force, and Navy are the top three spectrum users in the Federal Government. The FAA's numerous communication, navigation, and surveillance systems heavily depend on the RF spectrum, as evidenced by the agency's more than 50,000 frequency assignments.

Spectrum Management within the FAA ensures that systems that use RF technology are assigned proper frequency bands and do not degrade the performance of other RF systems within the NAS.

4.8.4.2.1 What Is Spectrum Management?

FAA Order 6050.19 states that "the radio spectrum is a scarce and limited resource" and that "the FAA is committed to new spectrum-efficient technologies and procedures to preserve this precious resource."

Spectrum Management includes distributing the FAA's share of the RF spectrum among NAS systems, integrating new RF technologies into the existing NAS, monitoring RF activity to ensure that NAS RF systems do not interfere with one another, and investigating external sources of RF Interference (RFI) that may degrade performance of NAS systems.

4.8.4.2.1.1 Coordination With Technical Operations Services

The Air Traffic Organization's (ATO) Office of Technical Operations Services (formerly Spectrum Policy and Management - ASR) oversees Spectrum Management within the FAA. All project teams developing systems that require RF usage shall coordinate with Technical Operations Services to ensure that all Spectrum Management issues are addressed correctly, including assigning RF bands. Project teams shall contact Technical Operations Services early in the development process and request guidance on spectrum issues.

Technical Operations Services manages FAA usage of the radio spectrum and resolves RFI issues by maintaining a network of Frequency Management Officers (FMOs). Nationally, FMOs are the aviation community's point of contact for resolving reported cases of RFI. Spectrum engineers assigned to the Regional Frequency Management Offices perform detailed onsite investigations to quickly resolve RFI cases to keep the NAS operating in an interference-free electromagnetic environment. FMOs can also engineer local or "site-specific" radio frequencies for approval by Technical Operations Services.

4.8.4.2.2 Why Perform Spectrum Management?

Spectrum Management applies only to systems that transmit RF signals. The following sections discuss the key reasons for incorporating Spectrum Management into the SE process.

4.8.4.2.2.1 Spectrum Management Is Required for All RF Systems

The U.S. Office of Spectrum Management assigns RF bands to government agencies and civilian industries. Federal law prohibits RF usage outside the assigned bands.

The ATO's Technical Operations Services oversees the FAA's assigned RF bands. It is *mandatory* for project teams developing RF systems to collaborate with Technical Operations Services to obtain specific RF band assignments.

Technical Operations Services continues Spectrum Management activities throughout a system's lifecycle (e.g., frequency reassignments, RFI investigations).

4.8.4.2.2.2 RF System Performance

Spectrum Management is necessary to maintain an interference-free environment for RF systems. Without Spectrum Management, RFI would be difficult to control, and the performance of RF systems would be seriously degraded. The limited number of usable existing frequency bands dictates the need to organize, coordinate, and monitor spectrum use.

4.8.4.2.3 Activities of Spectrum Management

Spectrum Management activities involve identifying and maintaining an RF system's transmission frequencies.

4.8.4.2.3.1 Initial RF Band Assignments

The ATO's Technical Operations Services will assign frequency bands for operational use with new NAS systems. A new RF system cannot be introduced into the NAS without obtaining frequency assignments.

4.8.4.2.3.2 RFI Detection and Reporting

New systems must be tested to ensure that they do not transmit noise that may interfere with other RF systems. Technical Operations Services can provide specific testing criteria.

Any external (unaccounted for) RFI that impedes a system's performance during operational use should be reported to the appropriate regional Frequency Management Officer for investigation.

4.8.4.2.3.3 RF Band Modifications

At any point during a system's lifecycle, Technical Operations Services may change frequency band assignments for any or all NAS systems. Reassignments may be needed because of integration of new RF systems into the NAS, changes in NAS customer needs, RF spectrum allotment adjustments made by the U.S. Office of Spectrum Management, or international issues. Band assignment modifications can occur on a local, national, or international level. Project teams and systems engineers must be prepared to make frequency band adjustments as required by Technical Operations Services.

4.8.4.2.4 Outputs and Products of Electromagnetic Environmental Effects

Figure 4.8-1 illustrates the fundamental Specialty Engineering process and its outputs. The following sections link the outputs of Spectrum Management activities to the overall System Engineering process. All Spectrum Management issues shall be addressed directly with Technical Operations Services.

4.8.4.2.4.1 Planning Criteria and Initial Requirements Document

During the early Mission Analysis stage, determining the need and submitting a request for spectrum support to Technical Operations Services is a priority for an RF system team. The initial requirements document process is not complete until the Spectrum Planning Subcommittee approves the request. The feedback from Technical Operations Services shall feed the Integrated Technical Planning process (Section 4.2) and the Requirements Management process (Section 4.3).

4.8.4.2.4.2 Requirements and Constraints

Technical Operations Services may impose requirements and/or constraints on an RF system at any stage of its lifecycle. These shall be used to feed the Requirements Management process (Section 4.3).

4.8.4.2.4.3 Verification Criteria

Technical Operations Services requires validation for any RF system under development that ensures spectrum usage of the system is within the approved bounds. This feeds the Validation and Verification process (Section 4.12).

4.8.4.3 References

For FAA-related subject matter expertise in E^3 and Spectrum Management, contact ATO's Office of Technical Operations Services. Additional sources of information on E^3 and Spectrum Management include:

4.8.4.3.1 Policy Guidelines

NTIA (2004), "Manual of Regulations and Procedures for Federal Radio Frequency Management (May 2003 Edition, 2004 Revision)," U.S. Department of Commerce, National Telecommunications and Information Administration, Washington, DC. http://www.ntia.doc.gov/osmhome/redbook/redbook.html.

DOT, "Radio Frequency Spectrum Use," DOT Order 5420.3, U.S. Department of Transportation, Washington, DC.

FAA (2000), "Radio Spectrum Planning," FAA Order 6050.19E, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 June.

FAA (2001), "Electronic Equipment, General Requirements," Section 3.3.2 "Electromagnetic Compatibility" FAA-G-2100G, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 22 October.

FAA (2002), "Radio Spectrum Plan 2001-2010 (2002 Revision)," U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 September. http://www.faa.gov/ats/aaf/asr/library/docs/RSP-2002.pdf.

FAA (1998), "Spectrum Management Regulations and Procedures Manual," FAA Order 6050.32A, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 01 May.

4.8.4.3.2 Testing Guidelines

RTCA (1997), "Environmental Conditions and Test Procedures for Airborne Equipment," (With Three Changes Issued), RTCA/DO-160D, RTCA, Inc., Washington, DC.

DoD, (1999), “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” MIL-STD-461E, U.S. Department of Defense, Washington, DC, 20 August.

SAE (1999), “Electromagnetic Interference Measurement Antennas; Standard Calibration Method,” ARP958, SAE International, Warrendale, PA, March. http://www.sae.org/

IEEE (1979), “IEEE Standard Test Procedures for Antennas,” IEEE Std-149-1979, Institute of Electrical and Electronics Engineers, New York, NY. (Reaffirmed in 2003), ISBN 1-5593-7609-0. http://www.ieee.org

IEEE (1998), “Electromagnetic Compatibility-Radiated Emission Measurements in Electromagnetic Interference (EMI) Control-Calibration of Antennas (9 kHz to 40 GHz),” IEEE C63.5-1998, Institute of Electrical and Electronics Engineers, New York, NY.

4.8.4.3.2 Web Sites

www.fcc.gov	FCC
standards.ieee.org	ANSI/IEEE
www.jsc.mil/jsce3/e3prg.asp	Joint Spectrum Center, E3 Engineering Support

4.8.5 Quality Engineering

Quality Engineering (QE), sometimes called Quality Assurance (QA), is a Specialty Engineering discipline within System Engineering.

4.8.5.1 What Is Quality Engineering?

QE is an objective analysis of all planned and systematic activities to ensure that a product or service fulfills requirements and is of the highest quality. This includes analysis of any proposed acquisition, from the Mission Analysis phase of the Acquisition Management System (AMS) through the Solution Implementation phase. Such analysis ensures that program Requirements (see Requirements Management (Section 4.3)), including the Service Level Mission Need (SLMN), are allocated properly to the physical architecture of the solution system (see Synthesis (Section 4.5)). Additionally, QE analysis evaluates a system's ability to meet its requirements and to mitigate product defects before production of the system begins. Further, QE analysis identifies development and deployment metrics to ensure that the system is designed and produced to provide maximum benefit to the stakeholders.

QE is also a philosophy and set of guiding principles that are the basis for a continuously improving organization. In recent years, QE has shifted toward designing quality into the product, rather than trying to inspect quality into a poor product after it has been produced.

Thus, QE has become a means of documenting how things will be done, and it should be addressed early in the AMS cycle. Early participation in the quality process at all levels of an organization helps to determine general, high-level quality requirements within the preliminary Program Requirements (pPR).

4.8.5.2 Why Perform Quality Engineering?

QE is performed to:

- Monitor quality within the FAA using ANSI/ISO/ASQ Q9001-2000, WI-200-01 "ASU-200 ISO 9001 Work Instructions Quality/Reliability Officer Guidebook." This is the Software Quality Assurance (SQA) Model of the FAA Air Traffic Organization (ATO), Operations Planning (ATO-P). (ATO-P is composed of many former organizations, including ASU-200.) The model is consistent with the FAA Integrated Capability Maturity Model (FAA iCMM).

- Reduce costs and improve product performance

- Comply with FAA Order 4630.8, "Quality Assurance Policy," and AMS paragraph 3.10.4

FAA Order 4630.8 requires the FAA to institute a quality program/system for National Airspace System (NAS) acquisitions of all systems, equipment, materials, and services. In the past, FAA-STDs-013, -016, and -018 quality specifications were placed on NAS programs. Currently, International Standards ANSI/ISO/ASQ Q9001-2000 are included in new NAS contracts to reflect advances in the quality sciences.

Specific requirements of AMS paragraph 3.10.4 can be easily accessed in the FAA Acquisition System Toolset (FAST) at http://fasteditapp.faa.gov/ams/do_action?do_action=LinkSection&contentUID=4&sectionNumber=3.10.4.

The FAA iCMM, v. 2.0 (see http://www.faa.gov/ipg/pif/icmm/index.cfm) describes characteristics for assessing efficient internal FAA processes. Process Area 15 (PA15) addresses Quality Assurance and Management. The FAA iCMM quality focus is to ensure the quality of the product or service, ensure the quality of the processes to generate or provide the product, and provide management visibility into the processes and products. However, the iCMM, as a high-level document, provides criteria to determine if quality is being met, but it does not contain the detailed process. This section provides that process.

In addition, the practice of QE promotes reduced costs and risks in upgrading the NAS. To some, this concept is contradictory. Many believe that improved quality only results from more inspection, which increases costs in both time and money. Others believe that it takes much longer to design and manufacture a higher quality product. Figure 4.8.5-1 (a) shows a balance between costs and defects, where moving to either side of that balanced position results in higher costs.

Many industries have proven these beliefs to be wrong. They have shown that inspection alone does not improve quality. In fact, many companies produce high-quality products at lower costs. Organizational focus throughout the lifecycle is what really resolves quality issues. By improving processes (see Figure 4.8.5-1 (b)), companies decrease defects while maintaining the same or lower costs; and decreasing product defects usually improves system performance and productivity. The net result is that stakeholders are more satisfied with the products or services.

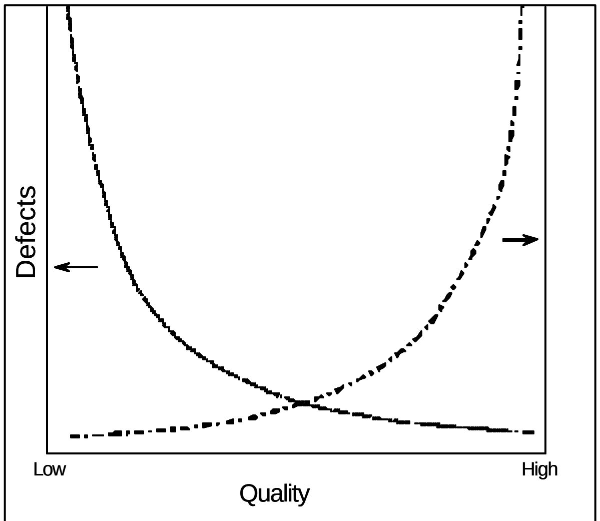


Fig. 4.8.5-1 (a) "Old cost vs. defect tradeoff"

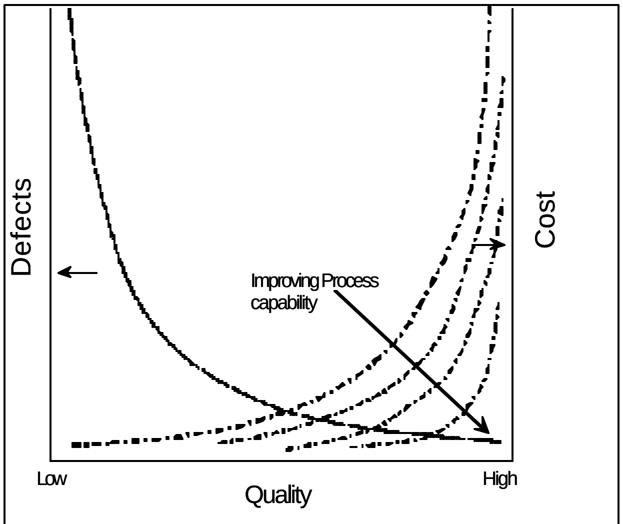


Fig. 4.8.5-1 (b) "New cost vs. defect tradeoff"

4.8.5.3 Quality Engineering Process Tasks

QE follows the basic process tasks outlined in "General Specialty Engineering Process Tasks" (subsection 4.8.0.3).

Additionally, for software quality assurance, there are specific process tasks in the "Software Quality Assurance and Industrial Evaluation Guidebook" (http://www.asu.faa.gov/ASU-200/QualitySystem/WH-250-01.doc). QE analysis supports the SLMN analysis, Investment Analysis Team, and the Service Organization. QE provides high-level quality plan recommendations during the Mission Analysis phase, but primarily participates in the Investment Analysis and Solution Implementation phases.

4.8.5.3.1 Mission Analysis Phase

QE involvement is at a macro level during the Mission Analysis phase. QE participates in developing or revising the SLMN. QE supplies estimates of quality costs to the system engineer member of the Service Level Mission Need Development Team, who shares these inputs with the team. Additionally, QE reads, reviews, and comments on the SLMN as it is developed, ensuring that QE concerns are expressed and documented. QE participates in the alternatives analysis, assisting in evaluating alternatives and commenting on technological feasibility of the alternatives, especially technological maturity. QE also contributes to the concept of use definitions, which may reflect back to the technological feasibility or interfaces of the proposed alternative. All these Mission Analysis activities contribute to development of the pPR, which is the Exhibit 300 Attachment 1.

4.8.5.3.2 Investment Analysis Phase

During Investment Analysis, the QE process reviews the pPR (to ensure that all QA requirements are included) and provides inputs to the Implementation Strategy and Planning (ISAP) (Exhibit 300 Attachment 3). These inputs include general descriptions of the QE philosophy, baseline quality requirements, and constraints concerning risk management. QE analysis outputs are provided to Requirements Management (Section 4.3), Integrated Technical Planning (Section 4.2), the Service Organization, and Investment Analysis Team.

4.8.5.3.2.1 Develop Acquisition Strategy

QE helps develop the overall strategy for implementing the acquisition program within the cost, schedule, performance, and benefit parameters of the program's Exhibit 300.

QE develops the QA section of the ISAP, and recommendations for the ISAP should include the following:

- Establish QA controls, including contractor status reporting, quality metrics, peer review, and independent verification and validation
- List QA standards with justification for selecting those quality standards
- Select automated tools used to manage and communicate QA actions and activities
- Ensure that the vendor's software Quality processes are evaluated and scored as a part of the source selection

- Monitor the vendor’s software Quality processes after award
- Establish Quality milestones
- Estimate Quality funding requirements by fiscal year
- Estimate appropriate Quality resources by fiscal year

Outputs and recommendations for ISAP should be provided in writing and copies of recommendations retained. Figure 4.8.5-2 is an example of a simple program support plan form.

Program Support Plan

SECTION A: *(Example)* **PROGRAM INFORMATION**

ANALYST: *(Name of Program Analyst)* Jane Q Engineer	**DATE:** *(Date prepared)* 01/01/2010
PROGRAM NAME and DESCRIPTION: *(Program name (acronym) and description)* Next Upgrade Backup System (NUBS)	
TYPE OF PROGRAM: *(Commercial-off-the shelf/non-developmental item, etc.)* Design/development	**EST. CONTRACT AWARD DATE:** *(Anticipated award date)* 06/06/2010
EST. CONTRACT END DATE: *(Anticipated end date)* 08/08/2015	**EST. SOFTWARE KSLOC:** *(Estimated thousands source lines of code)* 200 KSLOC
CAS CODE: *(Cost Accounting Standard Code)* 00010000	**EST. SOFTWARE CSCIS:** *(Estimated number of Computer Software Configuration Items)* 20

SECTION B: **PRE-AWARD INPUT AND ACTIVITIES** *(List pre-award input provided: i.e., document/review/evaluations/activity as applicable. Insert additional rows as necessary for each item.)*

INVESTMENT ANALYSIS: INPUT/ACTIVITY *(Example)*	COMMENTS	Due Date	Date Complete
Preliminary Program Requirements, Exhibit 300 Attachment 1	Review preliminary Program Requirements and provide comments to service organization	1/2010	

PROGRAM PLANNING: INPUT/ACTIVITY *(Example)*	COMMENTS	Due Date	Date Complete
Implementation Strategy and Planning	Prepare Quality Assurance section of ISAP and review and comment	1/2011	
Source Selection Plan	Prepare Quality Assurance portion of Source Selection Plan	3/2011	

SIR/CONTRACT: INPUT/ACTIVITY *(Example)*	COMMENTS	Due Date	Date Complete
Statement of Work (SOW)	Prepare Quality Assurance Section of SOW	2/2011	
Screening Information Request (SIR)	Prepare Quality Assurance Section of SIR	4/2011	
Contract	Prepare Quality Assurance portion of SIR, Section E, Quality Assurance Critical Design Review, and Data Item Descriptions	5/2011	

EVALUATION ACTIVITIES: INPUT/ACTIVITY *(Example)*	COMMENTS	Due Date	Date Complete
Review Quality Assurance Plans	Review and recommend actions regarding Quality System Plans	4/2011	
Review Software Quality Assurance Plans (SQAP)	Review and recommend actions regarding SQAPs	4/2011	
Review Test Plans	Review and comment	4/2011	

SECTION C: POST- AWARD MILESTONES/ACTIVITIES

MILESTONE/ACTIVITY *(Example)*	COMMENTS	Date Scheduled	Date Complete
POST-AWARD CONFERENCE:	Estimated to be within 1 month of contract award	TBD	
DESIGN REVIEWS:	Preliminary Design Review, Software Design Review, Final Design Review, and Functional Configuration Audit/Physical Configuration Audit	“	
TECHNICAL REVIEWS:	Technical Interchange Meetings, Code walkthroughs, and Test Readiness Reviews	“	
TESTS:	Design Quality Test, Factory Acceptance Test, and Site Acceptance	“	
DELIVERIES:	Initial delivery no later than 12 months after contract award — schedule per contract	“	
INSTALLATION:	Initial installation 16 months after contract award	“	

SECTION D: CONTRACT INFORMATION
(Example)

CONTRACT #: FA01-C-10- 000000	**$VALUE AT AWARD:** $80,000,000
CONTRACTOR: Acme Corp. **LOCATION:** Any City, OK	**TOTAL QUANTITY ORDERED:** 100 Systems
CONTRACT AWARD DATE: Estimated 6/2010	**TYPE OF CONTRACT:** Cost Plus Fixed Fee
ACCEPTANCE: Preliminary: QRO Source Final: Destination	**GOVERNMENT FURNISHED PROPERTY/CONTRACTOR ACQUIRED PROPERTY:** Next Upgrade Backup System NUBS Test Set

SECTION E: QRO STAFFING ESTIMATES
(Example)

FY: 2010	**QTR 1**	**QTR 2**	**QTR 3**	**QTR 4**	**YR 2**	**YR 3**	**YR 4**	**YR 5**	**YR 6**
Software	0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
Hardware	0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
TOTAL	0.00	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0

Figure 4.8.5-2. Sample Product Plan

4.8.5.3.2.2 Augment Program Work Breakdown Structure

QE helps to develop the program Work Breakdown Structure (WBS). The WBS is a logical, tailored arrangement of work elements needed to deliver systems, and it should be tailored to the acquisition program and clearly describe the product to be developed. One must be familiar with the WBS to understand the program’s technical objectives, specification tree, and configuration items.

4.8.5.3.2.3 Establish Program Metrics

Program metrics, including QA metrics, aid program management by identifying problems, measuring product quality, and assessing process conformance and effectiveness. QE determines the appropriate QA program metrics used to evaluate progress, monitor critical issues and risks, and provide information for cost and schedule estimates. Each metric should be related to and defined in terms of a specific process, risk factor, or key program element. Metrics should include descriptions; quantitative bounds; and the identity of the parties responsible for identifying, collecting, and analyzing data as well as for reporting the results of metrics analysis. Program metrics should be scaled appropriately to the overall program. As determined by QE, the metrics should include:

- A measurement action plan
- Risk management metrics
- Earned value management metrics
- Software design and development metrics

4.8.5.3.2.4 Contribute to Implementation Strategy and Planning, Exhibit 300 Attachment 3

The ISAP consists of all planned actions and activities, including QE actions and activities, to successfully complete the program. The ISAP's Quality Assurance section, at a minimum, includes Contractor Status Reporting, In-Plant Quality/Reliability Officers (QRO), Independent Validation and Verification, and Contractor Software Process Monitoring activities. QE activities need to be integrated into the system design, production, and deployment activity plans. There may be cost and schedule estimates that need to incorporate quality work efforts and tasks defined in the ISAP.

4.8.5.3.3 Solution Implementation Phase

Following the investment decision, QE participates in the acquisition strategy during the Solution Implementation Phase, which includes Contracting Support (see lower half of Table 4.8.5-1) and Post-Award Activities. The QE provides the bulk of the analysis during this time.

4.8.5.3.3.1 Contracting Support

The contracting stage of the Solution Implementation phase begins after the Final Investment Analysis Decision. Contracting covers all activities that lead to contract award, including preparing the Screening Information Request (SIR), evaluating offers, and selecting the source.

QE prepares the QA portions of the SIR, the Statement of Work (SOW), Contract Data Requirements Lists (CDRL), Data Item Descriptions (DID), Instructions to Offerors, and the contract itself. QE assists in developing the System Specification, Contract WBS, Evaluation Plan, and Selection Criteria. Additionally, QE evaluates offerors' proposals, providing recommendations to the source selection official for making the down-selection or award decision (see Table 4.8.5-1).

Table 4.8.5-1 QE Task/Products Aligned With Contract Phase

Solution Implementation Phase	
Pre-Contact Award	**QE Tasks or Products**
Prime Contract WBS	• Review WBS • Comment on program planning, control, communications, cost estimates, and schedules
System Specification	Evaluate and comment on considerations in these areas: • Functional • Operational • Technical
SIR	• SOW • CDRL • DIDs
Evaluation Criteria	Identify key characteristics that enable evaluators to distinguish between proposals: • Contractor Assessment Criteria: Soundness of Approach • Specific Criteria: Technical, cost, business, and program management
Evaluation Plan	Contribute to development of plan as needed, tailored to specific needs of the program
Proposal Evaluation	• Track changes to QA requirements • Review bidders' QA plans • Monitor changes to CDRL • Identify changes to DIDs
Post-Contract Award	
Transition	• Transition to assigned QRO • Facilitate communication between QRO and the service organization • Assist QRO with QA Plan • Attend Integrated Product Team meetings

4.8.5.3.3.1.1 Develop Prime Contract Work Breakdown Structure

The contract WBS identifies the program work activities to complete the program and partitions and assigns responsibility for completing the activities to contractors, in-house resources, and support contractors. The prime contract WBS covers software and hardware design and development, system test, integration, and installations and identifies the independent operational test and evaluation activities. QE reviews the WBS and comments on the program planning, control, communications, cost estimates, and schedules.

4.8.5.3.3.1.2 Review System Specification

The System Specification translates requirements in the high-level initial requirements document into physical system requirements that can be partitioned and allocated to specific hardware and software configuration items. In reviewing the System Specification, QE evaluates the functional, operational, and technical considerations of the program.

4.8.5.3.3.1.3 Develop and Refine Screening Information Request

The primary items included in the SIR are the SOW, CDRL, DIDs, instructions, conditions and notices to offerors, and evaluation criteria. QE provides input and recommendations on all of these items. QE relies on sound quality principles and past experience to tailor the Quality plan to fit program needs. Thus, the analysis should:

- Specify the appropriate Quality requirements (i.e., ISO-9000-2000 and FAA-STD-026A)
- Determine whether bidders should provide quality and SQA Plans
- Define the program-specific Contract Data Requirement for the Quality and SQA Plans
- Tailor the DIDs to convey requirements to the contractor

4.8.5.3.3.1.4 Form Evaluation Criteria

QE assists in establishing the evaluation criteria to select contractors. These criteria define the selection factors and formally communicate FAA requirements to industry. Evaluation criteria must contain clear and sufficient technical guidance so that the contractor knows how the system is to perform. Evaluation criteria are included in both the evaluation plan and solicitation and typically fall into two general types:

- Assessment criteria—to assess soundness of approach and compliance with requirements
- Specific criteria—to assess technical, cost, business, and program management capabilities

Evaluation criteria also address logistics support, quality assurance, configuration management facilities, and subcontracting. Requirements included in the evaluation criteria should have a clearly defined scope and be consistent, sufficiently detailed, and appropriate for the established program needs (see Requirements Management (Section 4.3)). The primary concern is to determine the appropriate Quality evaluation criteria for the program. The following should be considered:

- Adequacy of Quality Assurance and Software Quality Assurance Plans
- Evidence of the contractor’s ability to comply with recommended quality requirements
- Evidence of the contractor’s ability to comply with recommended software quality requirements
- Need for an evaluation of a contractor’s manufacturing capabilities
- Need to evaluate contractor’s process controls

- Need to conduct software capability estimate evaluation or some other evaluation methodology (e.g., Software Assurance, RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification")

Evaluation criteria comments and recommendations should focus on key characteristics that enable evaluators to distinguish among proposals.

4.8.5.3.3.1.5 Prepare Evaluation Plan

Working with the service organization, System Engineering helps develop an evaluation plan tailored to the specific needs of the acquisition. The plan identifies the source-selection official and members of the evaluation team(s); contains the source evaluation criteria; defines evaluation methods and processes; establishes the evaluation schedule; and contains any other information related to source selection. There should be a Quality representative on the evaluation team. The completed and approved plan must be completed before the SIR is released.

4.8.5.3.3.1.6 Prepare Screening Information Request for Prime Contract

A SIR solicits documentation from offerors that the service organization uses to identify the offeror that provides the government the best value. The documentation includes qualification information, screening information, and requests for offers, as well as presentations, proposals, or binding offers. The type and number of SIRs issued depend on the acquisition and the service organization's source-selection approach. SIR preparation activities may include:

- Reviewing and providing input to the proposed SOW
- Reviewing and commenting on the proposed System Specification
- Reviewing and commenting on the WBS
- Determining and recommending appropriate Quality Requirements (e.g., ISO 9001, etc.)
- Preparing Quality System program evaluation criteria for the SIR
- Reviewing the CDRL to determine the review and/or approval process
- Assisting the service organization in finalizing Test Requirements for the SIR
- Assisting the service organization in determining appropriate reliability requirements (see Requirements Management (Section 4.3))
- Preparing descriptions of additional screening elements (e.g., establishment and maintenance of contractor parts support depot) with the service organization

4.8.5.3.3.1.7 Evaluate Proposals for Prime Contract

QA capabilities of the bidders submitting proposals are critical to the service organization's evaluation of the proposals' validity. Proposal evaluation activities relating to Quality include:

- Evaluating any proposed changes to QA requirements
- Evaluating bidders' proposed QA plans
- Reviewing any proposed changes to CDRL items
- Reviewing any proposed changes to DIDs

4.8.5.3.3.2 Post-Award Activities

Following contract award, the contractors and subcontractors begin engineering and system integration activities to produce and field systems. The FAA oversees the contractor's work to ensure that the system being built meets functional and operational requirements and is installed, integrated, supported, and maintained throughout the system lifecycle. QE continues to support programs controlled by service organization following contract award; however, QE transfers the primary QA work to the QRO. This successful transition and continued service organization and QRO support are critical to the continuity of the Quality program in the acquisition process.

QE and the QRO must coordinate activities and establish effective working relationships within the service organization and with the contractor. To establish and maintain this relationship during System Development, QE must:

- Ensure transition of the program to the assigned QRO
- Facilitate communication between the QRO and the service organization
- Assist QRO with the QA program
- Participate in service organization weekly/biweekly meetings

4.8.5.3.3.2.1 Ensure Program Transition to Quality/Reliability Officer

QE must ensure transition of the program to the QRO to ensure smooth development of the FAA in-plant QA program. Transitioning activities include:

- Briefing the QRO on the program and Quality issues
- Ensuring that the QRO has all documents needed to help establish the FAA in-plant Quality system
- Introducing the QRO to the service organization

- Assisting in establishing a working relationship with the QRO, service organization, and the contractor

- Assisting the QRO in setting up the FAA Quality system

- Assisting the QRO in preparing and submitting recommendations to the contract officer and service organization for the contract, as well as contract requirement changes, such as further tailoring ISO requirements or changes to the Quality System Plan

- Providing tailored SQA Model Guidance for software-intensive programs

4.8.5.3.3.2.2 Support QRO–Service Organization Communication

QE attends service organization contract meetings to discuss quality-related issues and stay abreast of program developments.

Only QROs and individuals with specific delegated authority from the Contracting Office can deal directly with the contractor.

The group shares program information, including all reports and plans developed. The information exchange and coordination of efforts should be open, timely, and focused on supporting the service organization.

4.8.5.3.3.2.3 Assist QRO With Quality Assurance Plan

QE supports the assigned QRO, who inherited primary responsibility for the FAA Quality program, following contract award and transition of the FAA Quality program to the QRO. When requested by the QRO and service organization, QE assists in post-award activities.

4.8.5.4 Quality Engineering Outputs/Products

QE outputs consist of Design Analysis Reports, which support Mission Analysis, Investment Analysis, or Solution Implementation Phases. Additionally, the sample Program Support Plan (Figure 4.8.5-2) would be an output of the Investment Analysis Phase.

4.8.5.5 References

There are a variety of sources of information about Quality Engineering within the FAA, private industry, research institutions, and organizations and consortiums. The following subsections list books and documents and Internet sources that may further reader understanding of this process.

4.8.5.5.1 Books and Documents

1. *ASU-250 Software Quality Assurance and Industrial Evaluation Guidebook (WI-250-01)*. Washington DC: Federal Aviation Administration, 2002.

2. *International Council on Systems Engineering (INCOSE) System Engineering Handbook*. Version 2.0. Seattle, WA: INCOSE Central Office, 2002.

3. Martin, James N. *Systems Engineering Guidebook.* Boca Raton, FL: CRC Press LLC, 2000.

4. Sage, Andrew P., and Rouse, William B. *Handbook of Systems Engineering and Management*. New York, NY: John Wiley & Sons, Inc., 1999.

5. *Systems Engineering Capability EIA 731.* Electronic Industries Association, 1998, pages 79–81.

6. *The Federal Aviation Administration Integrated Capability Maturity Model® (FAA-iCMM®), Version 2.0.* Washington DC: Federal Aviation Administration, September 2001, specifically Process Area 15.

4.8.5.5.2 Web Sites

http://fast.faa.gov/: The Federal Aviation Administration Acquisition System Toolset; contains AMS Policy.

www.asq.org: The American Society for Quality, 600 North Plankinton Avenue, Milwaukee, WI 53203; or P.O. Box 3005, Milwaukee, WI 53201-3005.

www.qualitydigest.com: Quality Digest magazine online, Quality Digest, 40 Declaration Drive, Suite 100, Chico, CA 95973.

www.qualitymag.com: Quality Magazine, 1050 IL Route 83, Suite 200, Bensenville, IL 60106.

www.isixsigma.com: i Six Sigma; presents discussions and articles about process controls using Six Sigma methodologies.

4.8.6 Information Security Engineering

Information Security Engineering (ISE) is a specialty engineering discipline within System Engineering (SE). The practice of ISE **involves the analysis of threats and vulnerabilities to information systems and the assessment and mitigation of risk to the information assets that constitute the system during its lifecycle.**

Federal legislation, such as the Clinger-Cohen Act of 1996 and the Federal Information Security Management Act (FISMA) of 2002, establishes a clear legal basis for information security risk management of Federal information technology (IT) resources. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, establishes policy for managing Federal information resources and implements the law within the Executive Branch. Appendix III of Circular A-130, Security of Federal Automated Information Resources, establishes a minimum set of management controls for Federal programs. Appendix III defines Federal agency responsibilities for the security of automated information and requires that an agency official authorize operation of each IT system.

FAA Order 1370.82 has implemented OMB Appendix III by defining the Security Certification and Authorization Package (SCAP) as the basis for security authorization by the appropriate FAA official.

FAA Order 1370.82 states the FAA basic security policy:

> *The FAA shall ensure that security is provided commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information for all agency information collected, processed, transmitted, stored, or disseminated in FAA information systems and in information systems used on behalf of the FAA. The FAA shall also ensure that systems and applications used by or for the FAA provide appropriate confidentiality, integrity, authenticity, and availability.*

Further, the order describes roles and responsibilities related to certification and authorization (C&A) of IT products and systems within the FAA (e.g., Designated Approving Authority (DAA), Information System Security Manager (ISSM), or Certifying Agent (CA)).

The FAA procedures and practices for conducting ISE continue to evolve. This ISE section provides system/security engineers and program managers useful references, steps, and processes for effectively integrating Information Security into systems being developed and deployed, emphasizing assessment and mitigation of information security risks and the need to start early in the acquisition lifecycle.

4.8.6.1 Perform Information Security Engineering

In performing ISE, system and security engineers apply engineering principles to manage and control system security risk to the operational mission of the enterprise. The ISE process, outlined in subection 4.8.6.2, defines the tasks that will produce effective and suitable management, operational, and technical security controls for an FAA system. ISE is conducted during all phases of the system lifecycle. Security risk management, in conjunction with the security policies cited above, produce security requirements, which are statements of the implementation of mitigations to security risks that need to be controlled or reduced. Implementing system design and security controls mitigates security risks to an acceptable level. Successful application of ISE combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of a system's IT assets. IT assets include both data and information. The SE requirements management element (see Requirements Management (Section 4.3)) is essential for defining and implementing security controls.

Several factors drive the need to perform ISE and to develop and implement rigorous security controls. Figure 4.8.6-1 illustrates these drivers, which are:

- **Information Age Technology and Automation.** The FAA Acquisition Management System (AMS) calls for using or adapting commercially available IT products to satisfy the agency's mission needs. These commercial-off-the-shelf (COTS) products may contain vulnerabilities that, unless properly identified, controlled, and managed, could cause unacceptable risks to FAA services, capabilities, and functions.
- **Critical Infrastructure and Homeland Security.** Homeland Security Presidential Directive 7 **(**HSPD-7) establishes a national policy for Federal departments and agencies to identify and prioritize critical U.S. infrastructure and key resources and to protect them from terrorist attacks.
- **Aviation Growth—NAS Architecture and Operational Concepts.** The pervasiveness of networked information and the increased interconnectivity of FAA systems significantly broaden the agency's exposure to malicious activities from a variety of sources. Expanded services and capabilities that networking and automation have introduced enable improved performance and efficiency, yet dramatically expands vulnerabilities to systems' confidentiality, integrity, and availability unless the FAA properly addresses security.
- **Rising Terrorists and National Threats.** The FAA is modernizing its capabilities to ensure that the aviation transportation system is adequately protected from risks to the safety and security of the flying public. Information security supports homeland security, contingency response, and disaster recovery as services and capabilities of the NAS, which is a critical infrastructure for the United States.

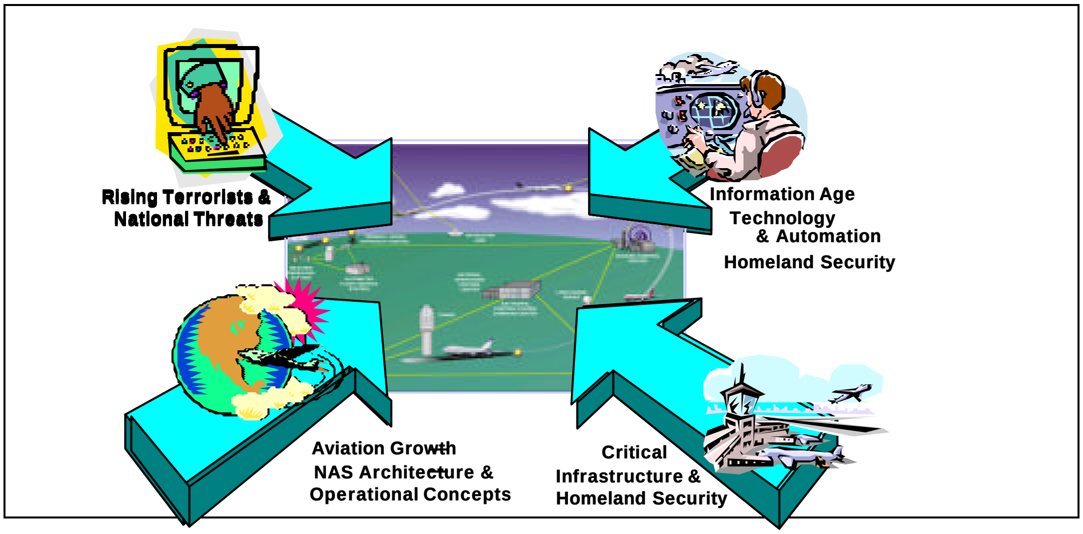


Figure 4.8.6-1. Force of Change Driving Security

These four factors drive the FAA toward more thorough and disciplined implementation of ISE throughout the system lifecycle. FAA programs that include security requirements early in development and acquisition typically have lower costs and more effective security features when compared to adding security controls later in the AMS lifecycle. The ISE process provides the information security risk management framework within the AMS, from early planning to contract closeout and/or system disposal.

4.8.6.1.1 Information Security Engineering Principles

ISE principles provide the foundation for a consistent and structured approach to designing, developing, and implementing information security capabilities that span the system both logically and physically. Applying ISE principles at appropriate phases of the system lifecycle can provide information security, which is a system characteristic. NIST[1] SP 800-27 identifies 33 ISE principles that should be considered during different phases of the system lifecycle. These principles are applicable across the system lifecycle, as summarized in Table 4.8.6-1, where one check (✓) signifies that the principle can be used to support the life-cycle phase, and two checks (✓✓) signify that the principle is key to successful completion of the lifecycle phase.

Table 4.8.6-1. IT Security Principles (from NIST SP 800-27) Versus AMS Lifecycle

IT Security Principles (NIST SP 800-27)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
1	Establish a sound security policy as the “foundation” for design.	vv	vv	v	v	v	v	v
2	Treat security as an integral part of the overall system design.	vv	vv	vv	vv	vv	vv	v
3	Clearly delineate the physical and logical security boundaries governed by associated security policies.	vv	vv	vv	vv	v	v	
4	Reduce risk to an acceptable level.	vv	vv	vv	vv	vv	vv	vv
5	Assume that external systems are insecure.	vv	vv	vv	vv	vv	vv	v
6	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.	vv	vv	vv	vv		vv	
7	Implement layered security (Ensure no single point of vulnerability).	v	v	vv	vv	v	vv	v
8	Implement tailored system security measures to meet organizational security goals.	v	v	vv	vv	v	vv	v
9	Strive for simplicity.	v	v	vv	vv	v	vv	v
10	Design and operate an IT system to limit vulnerability and to be resilient in response.	v	v	vv	vv		vv	
11	Minimize the system elements to be trusted.	v	v	vv	vv	v	vv	

[1] The National Institute of Standards and Technology (NIST) is a nonregulatory Federal Agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

IT Security Principles (NIST SP 800-27)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
12	*Implement security through a combination of measures distributed physically and logically.*			vv	vv	v	v	v
13	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.	v	v	vv	vv	v	vv	v
14	Limit or contain vulnerabilities.			vv	vv	v	v	
15	Formulate security measures to address multiple overlapping information domains.	v	v	vv	vv	v	v	
16	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).	v	v	vv	vv	v	v	
17	Use boundary mechanisms to separate computing systems and network infrastructures.			vv	vv	v	vv	
18	Where possible, base security on open standards for portability and interoperability.	v	v	vv	vv	v		
19	Use common language in developing security requirements.	vv	vv	vv	vv		vv	
20	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.	v	v	vv	vv	vv	v	
21	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.			vv	vv	v	vv	
22	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.	v	v	v	v	v	vv	
23	Use unique identities to ensure accountability.	v	v	v	v	v	vv	
24	Implement least privilege.	v	v	v	v	v	vv	
25	Do not implement unnecessary security mechanisms.	v	v	vv	vv	vv	v	
26	Protect information while being processed, in transit, and in storage.	v	v	vv	vv	v	vv	v
27	Strive for operational ease of use.	v	v	vv	vv	v	vv	
28	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.	v	v	v	v	v	vv	
29	Consider custom products to achieve adequate security.	v	v	vv	vv	v	v	
30	Ensure proper security in the shutdown or disposal of a system.			v	v		v	

IT Security Principles (NIST SP 800-27)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
31	Protect against all likely classes of "attacks."	v	v	vv	vv	vv	v	v
32	Identify and prevent common errors and vulnerabilities.			vv	vv			
33	Ensure that developers are trained in how to develop secure software.	vv	vv	vv	vv	v		

Subsection 4.8.6.3 (below) illustrates how ISE principles apply to the acquisition process and system lifecycle, including establishment of system-level security policy and integration of security into system design, which are two NIST SP 800-27 principles. Reducing information security risk to an acceptable level is a primary ISE principle. In today's networked world, the concept of risk management is central to ISE. Security risk management includes assessment, mitigation, monitoring, and control of security risks throughout the system lifecycle. The FAA defines information security risk as follows:

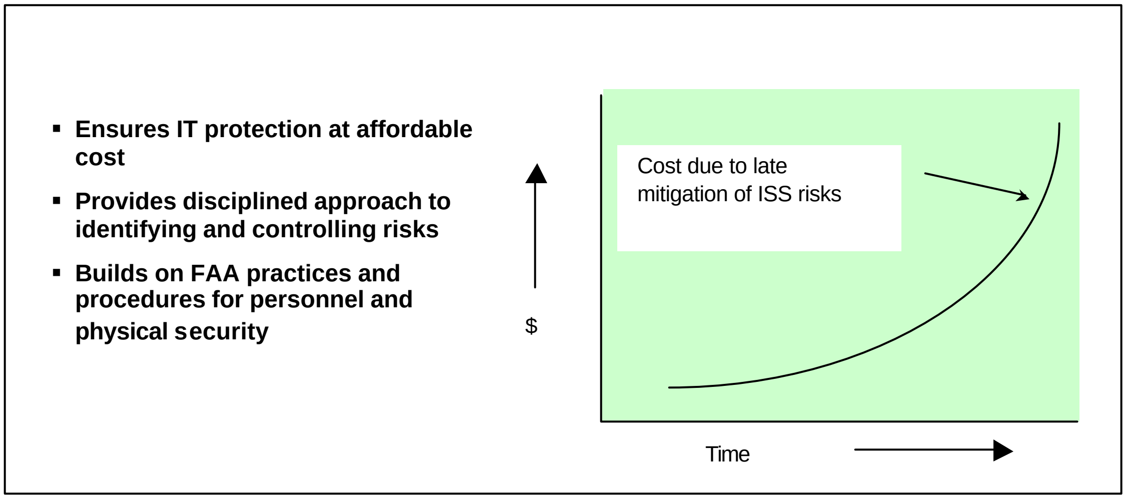
The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack.

Based on FAA Order 1370.82, the appropriate Designated Approving Authority (DAA) determines the acceptable level of risk based on a carefully considered risk assessment. The DAA determines whether the benefit of operating/connecting the system outweighs the residual risk, which is defined as the combined likelihood of exploits and potential loss or damage to mission capability. The DAA determination considers the operational benefits of the system, the criticality of information, the threats and vulnerabilities, and effectiveness of system features and security controls in addressing security risks.

Integrating system security into the design involves using the following ISE principles (as a minimum) during system development:

- (#8) Address the operational environment of the system and the system's contribution to the FAA mission and services in security policy
- (#3) Delineate clearly the physical and logical boundaries to be governed by the associated system security policies
- (#6) Identify potential tradeoffs between reducing risk and increased costs or impacts to operational effectiveness and suitability
- (#2–#31) Participate during Investment Analysis to identify security concerns and issues, assess system alternatives, and analyze security risks in alternatives. This ensures that the alternatives protect against likely classes of attacks.
- (#28) Include consideration of security features and controls for continuity of operations and disaster response to ensure appropriate availability

Participation in the Investment Analysis phase can improve security requirement statements and avoid costly, specialized controls for security services that may be effectively handled by existing system features, such as management procedures, operational controls, or boundary protection systems/services. Figure 4.8.6-2 illustrates the benefit of early ISE involvement in the system lifecycle.



- **Ensures IT protection at affordable cost**
- **Provides disciplined approach to identifying and controlling risks**
- **Builds on FAA practices and procedures for personnel and physical security**

Figure 4.8.6-2. Benefits of Early Information Security Engineering

Security risk management applies to every AMS phase. Subsection 4.8.6.2 (below) integrates guidance from NIST SP 800-30, Risk Management Guide for Information Technology Systems into the FAA Risk Management process model (Section 4.10). Table 4.8.6-2 indicates how risk management activities may be applied during the phases outlined in NIST SP 800-30, as well as the FAA AMS phases.

Table 4.8.6-2. Integration of Information Security Risk Management Into AMS

NIST SP 800-30 Phases	FAA AMS Phases	Support From Risk Management Activities
Phase 1 Initiation	Mission Analysis	Identified risks are used to support development of system requirements, including security requirements, and a security portion of the Concept of Operations (CONOPS).
Phase 2 Development or Acquisition	Investment Analysis	The risks identified during this phase are used to support the security analyses of the system alternatives that may lead to architecture and design tradeoffs during downstream system development.
Phase 3 Implementation	Solution Implementation	The security risk management efforts support assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks requiring mitigation must be made prior to system operation.

NIST SP 800-30 Phases	FAA AMS Phases	Support From Risk Management Activities
Phase 4 In-Service Management	Late stages of Solution Implementation and In-Service Management, including Technology Refresh	Risk management activities are performed for periodic system recertification and reauthorization, or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces).
Phase 5 Disposal	Service Life Extension	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

4.8.6.2 Information Security Inputs

As Figure 4.8.6-3 shows, several SE elements feed ISE. Functional Analysis, Requirements Management, Integrated Technical Planning, Interface Management, and Synthesis feed ISE with inputs, while Integrity of Analysis enables the ISE process. In turn, ISE provides output to other SE elements such as Functional Analysis, Requirements Management, and Risk Management. Note that ISE, like System Safety, conducts risk management separately from—yet it supports—Risk Management.

The ISE process outputs feed other SE processes, becoming integral to SE for the system life-cycle. Subsection 4.8.6.4 (below) details the ISE outputs and products, while subsection 4.8.6.3 discusses the ISE products that result from applying the ISE principles.

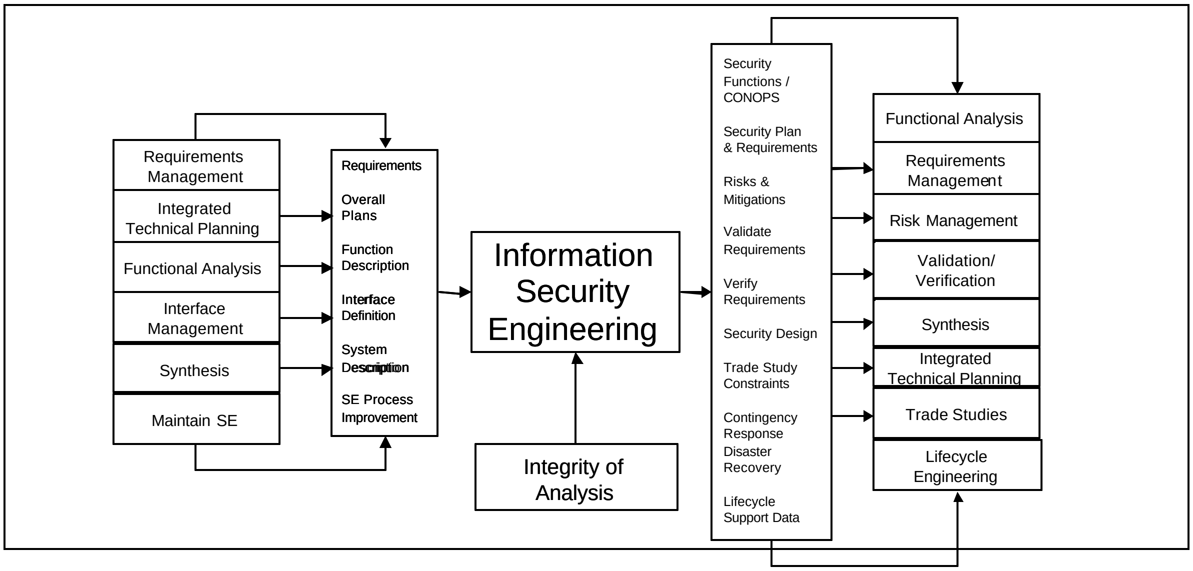
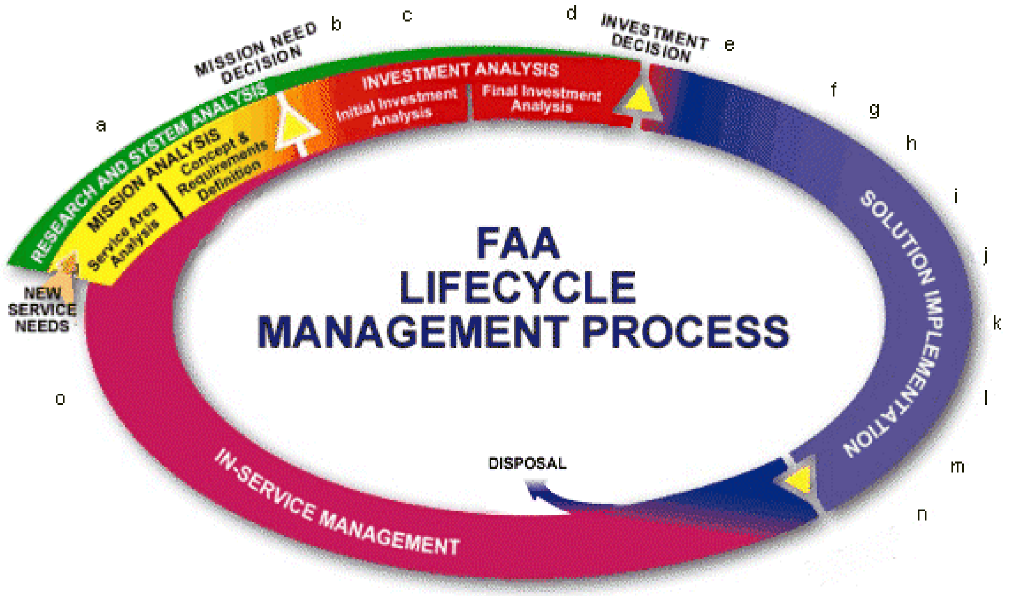


Figure 4.8.6-3. ISE Relationship to Other System Engineering Processes

4.8.6.3 Information Security Engineering Process Tasks

The ISE process tasks support the phased AMS decisions, as shown in Figure 4.8.6-4. Each program or Service Organization shall tailor its ISE activities to meet its program milestones and use its System Engineering Management Plan (SEMP) to tailor its ISE activities and process tasks.

Each phase has ISE products that support the other SE elements, consistent with Figure 4.8-1, “Specialty Engineering Process-Based Management Chart,” and subsection 4.8.0.3, “General Specialty Engineering Process Tasks” (in Section 4.8). The Information System Security Plan (ISSP) is a key ISE planning document for every FAA IT program. The ISSP provides an overview of the system, presents an approach for meeting associated security requirements, and delineates responsibilities and rules for controlling access and use of information and related assets within the system. The program ISSP is a living document, prepared early in the system lifecycle and updated regularly during program/system development. Table 4.8.6-4 summarizes the ISE process task alignment with the AMS phases.



Legend
ISE Risk Management Process Aligned With AMS

Numbered items correspond to AMS Lifecycle diagram numbers, above

a. Integrate Initial Security Needs and Threat Stipulation into MNS
b. Develop Preliminary ISSP including Basic Security Policy
c. Develop CONOPS and Preliminary Security Requirements
d. Develop Preliminary Vulnerability and Risk Assessment
e. Update Vulnerability and Risk Assessment
f. Update CONOPS and Security Requirements
g. Integrate Security Requirements with System Requirements
h. Integrate Security Architecture and Design
i. Update ISSP
j. Develop Security Test Plans and Procedures
k. Develop Users Guides, Training, and Contingency Plans
l. Conduct Security Testing
m. Create Final Security C&A Documents
n. Obtain Security Authorization/Accreditation
o. Prepare for Tech Refresh and Upgrade

Figure 4.8.6-4, ISE Process and the AMS Lifecycle Spiral

The following subsections summarize the ISE tasks for each AMS phase.

4.8.6.3.1 Mission Analysis Phase

The ISE process starts in Mission Analysis. In this phase, the ISE process focuses on the proposed system's operating environment, system boundaries, information assets and functions, and the potential threat and vulnerability sources to the system's information assets and functions. Basic system security policy flows from FAA organizational directives, such as FAA Order 1370.82, as well as from FAA operating procedures and instructions. Basic system security policy is the set of rules governing control, access, and use of system information. For example, a basic security policy statement may be that only authorized FAA users shall access the system. The ISE process applies Federal Information Processing Standards (FIPS) 199-1 to categorize system information assets and functions. The ISE process analyzes the system and NAS concept of operations (CONOPS) and mission need statement to formulate a basic security policy. The security planning aspects of ISE also begins in this phase, following guidance of NIST SP 800-18. Security requirements, based on security policy, are in the preliminary Program requirements document.

4.8.6.3.2 Investment Analysis Phase

Integrating the ISE process with SE elements is essential. During initial investment analysis, ISE develops and documents the security CONOPS and the initial security requirements for the initial Requirements Document. The investment analysis team uses the CONOPS and security requirements to evaluate system alternatives. Security engineers on the team conduct a preliminary risk assessment using updated threat and vulnerability data to determine specific risks that must be controlled/mitigated. Security trade studies are performed to evaluate system alternatives and to assess security risk controls/mitigation measures related to the system alternatives. Also, security trade studies identify native, existing system, and/or network features that reduce the likelihood of system threats successfully exploiting a vulnerability. These trade studies compare costs and benefits of system features/security controls in terms of risk reduction. Trade studies may evaluate the cost-effectiveness of different controls for a given risk or set of risks. Also, system alternatives may require different types of controls to balance system performance and security requirements against the security risks/costs of different alternatives. Different system alternatives may have significantly different physical and/or system architectures that would require different security controls, which lead to different security costs and effectiveness.

During the final stage of the Investment Analysis phase, ISE refines and updates the preliminary risk assessment. Updated threat and vulnerability data is applied, analyzing the costs and effectiveness of system features and security controls that are associated with each of the final system alternatives. ISE provides final security requirements for the final Program Requirements Document and the system specification, as well as special requirements for the Solicitation Information Request (SIR) and contract Statement of Work (SOW). In developing the final system requirements, ISE analyzes and establishes the appropriate assurance level to be proven during system implementation. Assurance in this context addresses the required level of confidence in the security function and performance and ensures that the security controls function in an integrated fashion. Assurance can be gained through many techniques, including conformance testing, independent verification testing, and employing diverse and/or redundant capability.

ISE shall support a documented agreement among FAA stakeholders regarding the necessity and sufficiency of the security requirements. Clearly documenting the agreement to security requirements before the Investment Decision becomes the foundation for the Security Certification and Authorization Package, which shall be completed before the In-Service

Decision. During the investment analysis, ISE identifies the technically qualified, senior FAA official who shall certify that the system security controls meet the minimum FAA/NAS ISS requirements (see DAA discussion in 4.8.6 above). The ISSP, which was based on NIST SP 800-18 and was a conceptual draft during the Mission Need phase, is updated to become an initial draft.

The ISE products from this phase include the updated preliminary risk assessment, final security requirements, security trade studies to support cost-benefit/investment analysis of security controls, and input to the SIR, SOW, system specification, and Contract Data Requirements List (CDRL) for systems to be acquired. These products support the AMS milestone decision for transition into the Solution Implementation phase.

4.8.6.3.3 Solution Implementation Phase

The ISE activities during earlier phases provide the basis for updating, monitoring, and controlling system security risks and the respective mitigation measures or controls that are implemented during this phase of system development. A summary of ISE activities for this phase includes the following:

- Revise the security CONOPS and security requirements based on functional analysis performed during early stages of the Solution Implementation phase.
- Analyze the physical/system architecture, resulting in an allocation of the security features to be implemented in the system under development. Security trade studies may be needed to identify the appropriate security controls to be implemented that balance system and security requirements.
- Integrate the security features into the security architecture to balance them with the system architecture and design. Security trade studies, interface security requirements, and other SE outputs contribute to successful integration of security architecture into system design. System design reviews are key milestones for ensuring that security controls are integrated into system development.
- Update the ISSP based on the expected ISS functional and assurance controls derived from the system architecture and design. Refine system test planning and procedures to ensure that all security requirements and controls are addressed. The ISSP supports Validation (Section 4.12,subsection 4.12.1) and Synthesis (Section 4.5) to assess controls and assurance as being cost effective and meeting the ISS requirements. Use Risk Management (Section 4.10) and Requirements Management (Section 4.3) to mitigate security risk to acceptable levels. The criticality/sensitivity of the system and its information assets guides the type and level of controls and testing.
- Develop a users guide, training plans, and contingency/disaster recovery plans. Security procedures, rules, training, and planning for contingency and disaster recovery operations may be integrated into the integrated logistics support and lifecycle planning for systems.
- Conduct security testing. Security controls and mechanisms may be tested incrementally and as a part of system development testing. For mission-critical systems, a third party shall conduct independent testing of system vulnerabilities.
- Create final security Certification and Authorization (C&A) documents. The results of ISE activities—including relevant results from related SE elements such as Integrated Technical Planning (Section 4.2), Synthesis (Section 4.5), Validation and Verification (Section 4.12), and Lifecycle Engineering (Section 4.13)—shall be

considered as final security C&A documents. The Air Traffic Organization provides templates for collecting and presenting C&A documentation.

4.8.6.3.4 In-Service Management Phase

Activities during this phase include the following:

- Obtain security C&A. Stakeholder C&A review shall ensure that the DAA is in a position to certify and authorize the system as meeting security requirements and as presenting an acceptable risk to the FAA mission and NAS operations.
- Conduct performance measurement, monitoring, and reporting of security controls and incidents. Ensure that monitoring of ISS performance and assurance for the respective NAS service/capability has not degraded and that new vulnerabilities have not been introduced to the operational system.
- Update the C&A package to reflect any major configuration changes at least every 3 years, assessing changes in the environment and system for previously unforeseen risks from new threats and vulnerabilities. Plan and take corrective action as necessary.
- For disposal of the system, the following types of activities may be addressed in the Information System Security Plan, and conducted at the appropriate stage of the System Development Lifecycle
    - Archive Information—retain information as necessary, keeping in mind legal requirements and future technology changes that render the retrieval method obsolete.
    - Sanitize Media—ensure data is deleted, erased, or written over as necessary.
    - Dispose of Hardware and Software—dispose of the hardware and software in accordance with ISS policy.

Table 4.8.6-3 relates the required C&A package to the ISE process steps that provide the conceptual, initial, draft, update, and final results for the C&A package.

Table 4.8.6-3. Security Certification and Authorization Documents Related to Information Security Engineering Process

SCAP Documentation	ISE Process Source	How To Reference
System Characterization	ISE h, Draft ISE i, Draft	Security Risk Assessment Methodology and System Characterization Template
Information System Security Plan	ISE b, Conceptual ISE d, Draft ISE i, Update ISE m, Final	Security Risk Assessment Methodology and ISSP Template
Risk Assessment Report (Includes Threat and Vulnerability Assessments)	ISE d, Initial ISE e, Update ISE m, Final	Security Risk Assessment Methodology and Risk Assessment Report Template
Security Test Plan and Test Results Report	ISE e, Initial ISE g, Draft ISE j, Update ISE m, Final	Security Risk Assessment Methodology and Security Test Plan and Test Results Template
Risk Mitigation/Remediation Plan	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and Risk Mitigation/Remediation Plan Template
Contingency/Disaster Recovery Plan	ISE i, Initial ISE k, Draft ISE m, Final	Security Risk Assessment Methodology and Contingency/Disaster Recovery Plan Template
Executive Summary	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and Executive Summary Template
C&A Certificate	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and C&A Statement Template

4.8.6.4 Information Security Engineering Outputs/Products

The important aspect of security outputs/products is to embed security into the program products where possible to minimize treating security as a “standalone” component. The ISE process generates the following output and products.

4.8.6.4.1 Information System Security Plan (ISSP)

The system owner (Information Systems Security Certifier) or Service Level Mission Need (SLMN) sponsor shall initiate the ISSP during mission needs analysis. The ISSP evolves during the system’s lifecycle, driven by the progression of system development. The ISSP is updated and revised based on ISE activities or other SE activities. To further guide planning, Table 4.8.6-4 relates the ISE activities and products to both the AMS milestone products and SE products. Analysis products outlined in subsection 4.8.6.4.2 below are used to update the ISSP.

Table 4.8.6-4. Acquisition Management, System Engineering, and Information Security Engineering Relationship

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Initial requirements, Initial functional architecture, Threat analysis criteria, OSA	ISE a. Integrate Initial Security Needs and Threat Stipulation into the SLMN	Statement of security policy and threat environment stipulation	• New/updated SLMN • Draft pPR, including the concept of use; • Initial investment analysis plan • System Investment Analysis Review
			Requirements Management, Functional Analysis, Synthesis
CONOPS, Initial requirements, analysis criteria, OSA	ISE b. Develop CONOPS and Preliminary Security Requirements	Initial Security requirements, CONOPS	• Business case analysis report • Updated pPR for each alternative under serious consideration • Initial investment analysis plan • Acquisition strategy in the ISAP for each alternative under serious consideration
			Requirements Management, Functional Analysis, Conceptual functional architecture, Synthesis, ITP
FAA Policy, Standards, NAS Architecture, OSED, CONOPS	ISE c. Develop Preliminary ISSP (Including Basic Security Policy)	Preliminary ISSP with security policy statement	• Final SLMN • CONOPS • Final Investment Analysis Plan • Initial description of alternatives
			Requirements Management, Functional Analysis, RVCD, Trade Studies, Interface Management, SEMP

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
CONOPS, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	ISE d. Develop Preliminary Vulnerability and Risk Assessment	Preliminary Vulnerability and Risk Assessment	• fPR • Final investment analysis report • Final Exhibit 300 • Final ISAP
			Requirements Management, RVCD, VRTM, OSED, Specialty Engineering, Risk Management, Validation, SEMP
CONOPS, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	ISE e. Update the Vulnerability and Risk Assessment	Updated Vulnerability and Risk Assessment	• SIR • System Specification • SOW • CDRL • Source selection criteria and plan
			Requirements Management, Specialty Engineering, Risk Management, Validation
CONOPS, Initial requirements, analysis criteria, OSA	ISE f. Update the CONOPS and Security Requirements	Updated Security requirements, Updated CONOPS	Requirements Management, Functional Analysis, Trade Studies, Interface Management, Configuration Management
CONOPS, Final Security requirements, Security concept of use	ISE g. Integrate Security Requirements with System Requirements	Initial Verification Requirements Traceability Matrix, Interface Requirements Documents	• System Requirements Review • System Design Review – PDR
			Requirements Management, Integrated Technical Planning, Trade Studies, Synthesis, Interface Management, Configuration Management, Risk Management

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Physical Architecture, Final Security Requirements, Design Analysis Report, Functional Architecture	ISE h. Integrate Security Architecture and Design	Updated Physical Architecture, Functional Architecture	• System Design Review — CDR • System Capability Demonstration
			ITP, Requirements Management, Functional Analysis, Synthesis, Interface Management, Risk Management, Configuration Management
Physical Architecture, Functional Architecture, Risk Mitigation Plan, Updated Baselines, Updated CONOPS, FAA Policy, Interface Control Documents, Program Risk Summary	ISE i. Update the ISSP	Updated Information System Security Plan	• ISAP • Integrated Lifecycle Plan • System Test Plan • OT&E Plan
			ITP, Specialty Engineering, Configuration Management, Lifecycle Engineering
Verification Requirements, Traceability	ISE j. Develop Security Test Plans and	Security Test Plan, Security Test Procedures	• System Test Plan • OT&E Plan

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Matrix, Risk Mitigation Plans, Interface Control Documents, Test and Assessment Articles, Physical Architecture, Functional Architecture, Functional Specification, Master Verification Plan	Procedures		• Integrated Technical Planning, Requirements Management, Interface Management, Verification, RVCD, VRTM
Trade Study Reports, Operational Services and Environmental Description, Functional Specification, Government and International Regulations and Statutes, FAA Policy, Requirements	ISE k. Develop User's Guides, Training, and Contingency Plans	Contingency and Disaster Recovery Plan, User's Guides, Security Awareness Training (see 4.14)	• Integrated Lifecycle Plan • Functional Configuration Audit • Physical Configuration Audit
			Functional Analysis, Configuration Management, Trade Studies, Specialty Engineering, Verification, ITP
Updated Verification Requirements Traceability Matrix,	ISE l. Conduct Security Testing	Updated Risk Mitigation Plan, Security Test Report	• Test Readiness Review • Qualification Test • Final Acceptance Test • Site Acceptance Test

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Requirements Verification Compliance Document, Verification Criteria, Updated Master Verification Plan			Verification, Integrated Technical Planning, Requirements Management, Configuration Management, Risk Management
Risk Mitigation Plan, Program Risk Summary, Updated ISSP, Contingency Plans, Test Validation Reports,	ISE m. Create Final Security C&A Documents	Certification Package	• In-Service Review Checklist • OT&E Report Specialty Engineering, Configuration Management, Synthesis, Risk Management
Certification Package, FAA Management Decisions, Government and International Regulations and Statutes	ISE n. Obtain Security Authorization/ Accreditation	Finalized Certification Package	Specialty Engineering, Configuration Management, Synthesis, Risk Management
Validated Need, Stakeholder Needs, Integrated Lifecycle Plan, Updated Acquisition Program Baseline, External Environmental Forces	ISE o. Prepare for Tech Refresh and Upgrade Planning	Updated Security Requirements, Updated Security Certification Package, Updated Vulnerability and Risk Assessment	Lifecycle Engineering, Trade Studies, Configuration Management, Risk Management, Functional Analysis

4.8.6.4.2 Analysis Products

The risk assessment methodology described in this section guides collection of security analysis results and recommendations into products that support security accreditation of the service/domain/system. This methodology illustrates how ISE work products are used to validate and verify the security requirements of a given system. The work products are generated according to the individual ISSP for each FAA service/domain/system. Figure 4.8.6-5 indicates the type of closed-loop security risk management that is applied during the AMS phases consistent with FAA ISS Policy Order 1370.82.

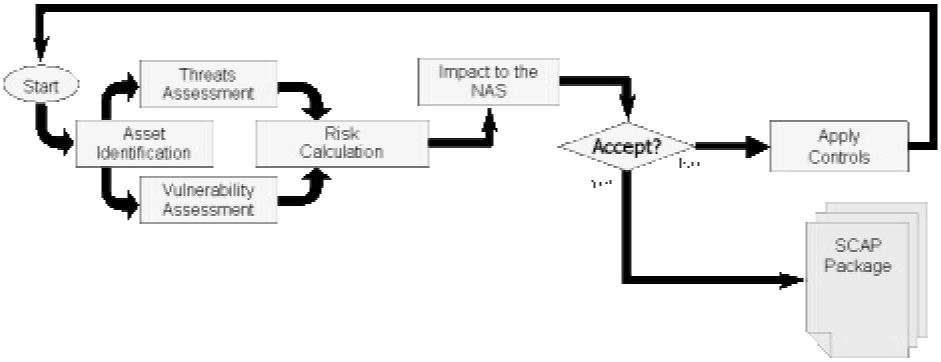


Figure 4.8.6-5. Closed-Loop Security Risk Management

This closed-loop method of risk management supports the FAA risk management process model described in Risk Management (Section 4.10), as shown in Figure 4.8.6-6 below.

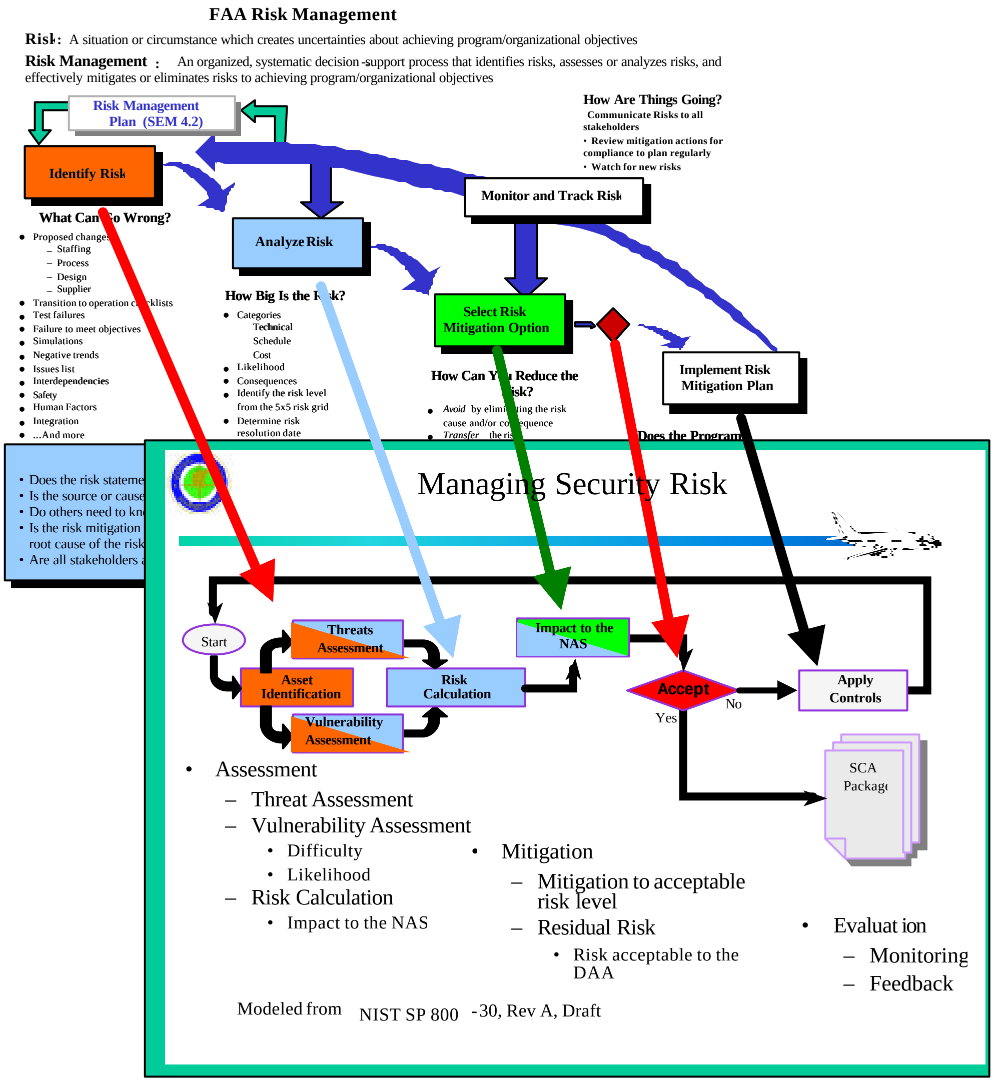

FAA Risk Management
Risk: A situation or circumstance which creates uncertainties about achieving program/organizational objectives
Risk Management : An organized, systematic decision -support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieving program/organizational objectives
Risk Management Plan (SEM 4.2)
Identify Risk
What Can Go Wrong?
Proposed changes
Staffing
Process
Design
Supplier
Transition to operation checklists
Test failures
Failure to meet objectives
Simulations
Negative trends
Issues list
Interdependencies
Safety
Human Factors
Integration
...And more
Analyze Risk
How Big Is the Risk?
Categories
Technical
Schedule
Cost
Likelihood
Consequences
Identify the risk level from the 5x5 risk grid
Determine risk resolution date
Monitor and Track Risk
How Are Things Going?
Communicate Risks to all stakeholders
Review mitigation actions for compliance to plan regularly
Watch for new risks
Select Risk Mitigation Option
How Can You Reduce the Risk?
Avoid by eliminating the risk cause and/or consequence
Transfer the ris
Implement Risk Mitigation Plan
Does the Program
Does the risk stateme
Is the source or cause
Do others need to kn
Is the risk mitigation root cause of the risk
Are all stakeholders a
Managing Security Risk
Start
Threats Assessment
Asset Identification
Vulnerability Assessment
Risk Calculation
Impact to the NAS
Accept
Yes
No
Apply Controls
SCA Package
Assessment
Threat Assessment
Vulnerability Assessment
Difficulty
Likelihood
Risk Calculation
Impact to the NAS
Mitigation
Mitigation to acceptable risk level
Residual Risk
Risk acceptable to the DAA
Evaluat ion
Monitoring
Feedback
Modeled from NIST SP 800 -30, Rev A, Draft

Figure 4.8.6-6. Correlation of Information Security Methodology With FAA Risk Management Model

The ISE Risk Assessment Matrix (Figure 4.8.6-7) can be used to analyze individual security risks. The matrix reflects the level of risk associated with the **likelihood** of a given threat source exploiting a given vulnerability and the **impact** of that threat source successfully exploiting the vulnerability. Risks to IT systems arise from events such as, but not limited to, the following:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors and omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT system

To use the matrix, apply the determined **likelihood** value generated for each threat-vulnerability pair and apply the **impact** rating, considering the vulnerability is successfully exploited. Locate the **likelihood** value in the vertical column and the **impact** rating in the horizontal column. The **Risk Level** is where the two values intersect.

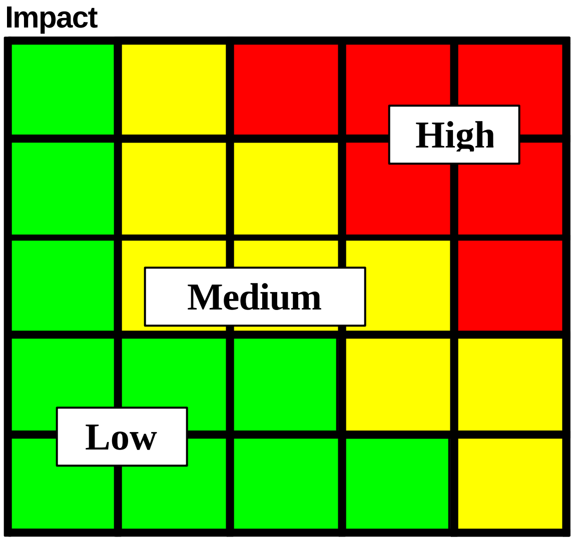


Figure 4.8.6-7. ISE Risk Assessment Matrix

4.8.6.5 Information Security Engineering Tools

There is not one specific set of tools for use in implementing Information Security. Tools should be chosen based on the desired final products and interoperability with other tools used in other SE elements. Tools can be used for discovering vulnerabilities, performing risk assessments, and for tracking and reporting the status of security controls.

4.8.6.6 Information Security Engineering Metrics

Reserved.

4.8.6.7 References

1. Clinger-Cohen Act of 1996.
2. FAA Order 1370.82, *Information Systems Security Program.*
3. Federal Information Security Management Act (FISMA) of 2002.
4. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems.*
5. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems.*
6. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems.*
7. NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security).*
8. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems.*
9. OMB Circular A-130*, Management of Federal Information Resources.*
10. OMB Circular A-130, *Appendix III, Security of Federal Automated Information Resources.*

4.8.7 Hazardous Materials Management/Environmental Engineering

Hazardous Material Management/Environmental Engineering (HMM/EE) is the subset of Specialty Engineering concerned with the impacts of both the program on the environment and the environment on the program. Federal, state, and local environmental agencies have established mandates that regulate program impacts on the environment. These mandates include requirements to manage hazardous materials and to safeguard natural resources including ambient air, water, and land-based resources. FAA orders and directives (e.g., FAA Order 1050.10, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities) relate Federal environmental regulations to FAA activities and also provide additional environmental requirements specific to NAS operations. Conversely, environmental impacts on programs vary, depending on site-specific environmental conditions that may affect FAA operational requirements. The following sections describe the purpose and general process of HMM/EE within SE.

4.8.7.1 What Is Hazardous Material Management/Environmental Engineering?

HMM/EE is the mechanism applied within the SE process to ensure a program's ongoing compliance with applicable environmental laws. HMM/EE is also the SE process designed to provide early, predeployment planning and coordination to minimize the negative impacts that site-specific environmental conditions may have on a program's operability. Compliance with various environmental regulations is required throughout a program's lifecycle, requiring early and continuous application of HMM/EE principles.

Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. It is recommended that additional issues concerning the applicability of state and local agency requirements to federal agencies be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications. For example, the National Environmental Policy Act requires preparation of an environmental assessment for all proposed federal actions that are not categorically excluded.

Additionally, the Resource Conservation and Recovery Act delineates standards for managing and disposing of hazardous wastes that result from various processes during program operation, and at the end of the program's lifecycle. Through HMM/EE, the breadth of environmental requirements are continuously monitored and considered to ensure that FAA's programs take the steps to maintain compliance.

HMM/EE processes also highlight the impacts that environmental conditions and site-specific characteristics may have on a program. FAA specifications developed for various types of equipment delineate operating conditions that shall be considered during the program's developmental stages. For example, the general FAA specification for electronic equipment, FAA-G-2100, details the design standards that shall be followed to ensure equipment functionality in environmental conditions of both seismic zones and temperature extremes. HMM/EE verifies that similar standards are considered and adhered to in the SE process to ensure the reliability of systems fielded under unique environmental settings.

4.8.7.2 Why Perform Hazardous Material Management/Environmental Engineering?

HMM/EE is performed to:

- Support reliable, safe, and sustained NAS operations

- Ensure that compliance with FAA, federal, state, and local environmental requirements

- Ensure environmental considerations are included in the acquisition management process

- Track the status of environmental issues with new and existing systems

- Minimize cost and schedule risks through early detection of environmental issues

Through various regulations, such as FAA Order 1050.17, Airway Facilities Environmental and Safety Compliance Program, the FAA has mandated and delineated requirements to comply with applicable environmental regulations. The FAA Acquisition Toolset System (FAST) ensures that these regulations are considered in the acquisition process in AMS Section 2.9.8, Environmental, Occupational Safety and Health, and Energy Considerations:

> *FAA acquisitions are subject to federal environmental, occupational safety and health, and energy management statutes, regulations, executive orders, and Presidential memoranda. Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. Additional issues concerning the applicability of state and local agency requirements to federal agencies should be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications.*

The following illustrate some of the requirements:

- The National Environmental Policy Act "requires preparation of an environmental assessment or an environmental impact statement for all proposed federal actions that are not categorically excluded. Depending on the results, an environmental assessment can lead to an environmental impact statement or a finding of no significant impact. Following the prescribed review periods, the FAA may make a decision on the federal action."

- Various other environmental laws (e.g., the Federal Facilities Compliance Act) "impose environmental requirements, and sanctions for noncompliance, including civil penalties."

- The Occupational Safety and Health Administration (OSHA) "requires a safe and healthful workplace for all employees, and compliance with OSHA standards."

  > *OSHA (29 CFR §1910.28) and GSA (Federal Property Management Regulations) require the FAA to establish and maintain an Occupant Emergency Plan for all FAA facilities. In the event an acquisition program impacts egress routes or fire safety of a facility, the plan must be updated by the program office or the Product Team performing the project.*

- The National Energy Conservation Policy Act "requires energy and water conservation measures for federal buildings, facilities or space."

> *Environmental, safety and health, and energy conservation considerations apply from the beginning of the acquisition lifecycle through product disposal. The Acquisition Program Baseline shall incorporate estimates for the full cost of complying and allow sufficient time for doing so. FAST contains procedural guidance for required actions*

When applied early, HMM/EE identifies applicable environmental requirements to include in development and acquisition of new systems, thereby providing significant savings through risk minimization, cost avoidance, and enhancement of system efficiency. Additionally, consideration of environmental impacts on systems while they are in the developmental stages ensures their functionality in various field conditions.

HMM/EE conducted as part of in-service program management analyzes the impact that engineering changes in the field may have on environmental concerns. As obsolete equipment is removed, HMM/EE ensures that replacement equipment complies with applicable environmental regulations. In particular, decommissioning and removal of obsolete equipment require HMM/EE considerations to ensure that final disposition/disposal is conducted in accordance with applicable environmental requirements. HMM/EE also evaluates the impact that regulatory changes may have on fielded systems.

Programs that fail to fully incorporate HMM/EE principles may have significant impacts on NAS operations. Noncompliant programs may:

- Be removed from service through regulatory enforcement actions
- Require costly post-fielding/retrofit modifications
- Incur fines

Additionally, costs associated with new equipment fielding, and obsolete equipment disposition and disposal may lead to significant budgeting issues if they are not considered during the program development phase.

4.8.7.3 Hazardous Material Management/Environmental Engineering Process Tasks

HMM/EE follows the process tasks outlined in General Specialty Engineering Process Tasks (subsection 4.8.0.3).

4.8.7.4 Hazardous Material Management/Environmental Engineering Outputs and Products

Throughout the various phases of the system acquisition process, HMM/EE is used in developing and reviewing key documents. Early implementation of HMM/EE principles is essential to minimize the impact that environmental requirements may have on system costs and operations. During the preliminary activities, such as development of mission needs, requirements, and investment analysis, HMM/EE is used to make initial assumptions and estimates on how environmental considerations may come into play throughout the various lifecycle stages.

During the solution implementation phase of the acquisition process, HMM/EE is used to shape portions of the SOW and system specifications documents as they relate to environmental considerations. For example, SOWs may be developed to support FAA efforts to meet National Environmental Policy Act demands that federal agencies minimize use of toxic substances in its operations.

During the in-service management phase of the system lifecycle, HMM/EE is used to address issues that may arise unexpectedly in the field. In particular, older pieces of equipment that may not have been developed with HMM/EE in mind may require corrective measures to meet environmental regulations. Additionally, the set of ever-changing environmental regulations may impact the way systems are operated. Finally, as old systems are decommissioned, HMM/EE is necessary to ensure that all disposal actions consider applicable environmental laws.

4.8.7.4.1 Program Integration

As part of the SE process, HMM/EE provides expertise for developing various documents required for program integration. Throughout the various lifecycle phases, HMM/EE ensures that all applicable regulations and environmental conditions are properly addressed so that their impacts are accounted for appropriately. For example, HMM/EE would support development of the IRD, keeping in mind environmental regulations that require federal agencies to verify that their activities do not negatively impact certain ecosystems. Similarly, HMM/EE's role in developing IPPs, SOWs, Disposition/Disposal Plans, and other such documents generates comments and input concerning the compliance requirements that may impact the progress of program implementation, and FAA's compliance status and future liabilities.

Included in the HMM/EE aspects of program integration is a functional analysis of the OSED (see Section 4.4 (Functional Analysis)). This portion of the functional analysis ensures that the environmental conditions that the various systems face are fully considered and that plans are appropriately developed to address identified conditions. Figure 4.8.7-1 depicts HMM/EE Inputs and Outputs.

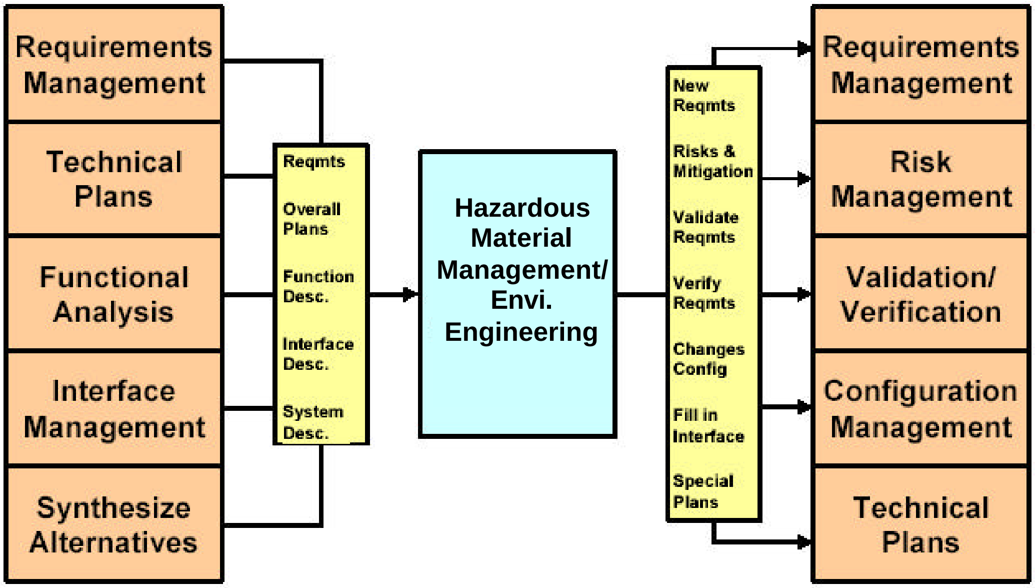


Figure 4.8.7-1. HMM/EE's Relationship to Other System Engineering Processes

4.8.7.4.2 Program Planning

FAA Order 1050.17 Airway Facilities Environmental Compliance Program implements the overall program for environmental compliance at FAA facilities. Each Region in the FAA has an Environmental Compliance Plan (ECP). The ECP is designed to identify and address compliance requirements in 19 environmental areas for all facilities, and therefore all systems within a region.

In addition to FAA Order 1050.17, FAA Order 4200.2, Utilization and Disposal of Excess and Surplus Personal Property, and AMS Section 2.8, Removing an Obsolete Solution, provide the requirements and framework for developing and implementing system-specific disposal plans for obsolete systems. These disposal plans are part of the Integrated Program Plan appendices; see subsection 4.2.2.1, “Introduction to the Integrated Program Plan”, in Section 4.2, Integrated Technical Planning.

4.8.7.4.3 Products

Additionally, it is recommended that, through the HMM/EE process, a program have the capability to produce an inventory of the hazardous materials fielded equipment may contain. This information has many purposes, including, but not limited to:

- Ensuring protection of the environment and surrounding communities
- Ensuring regulatory compliance during the program's operational life
- Supporting the safety of personnel working with equipment

- Supporting disposition/disposal efforts when obsolete equipment is removed from service

4.8.7.5 References

1. *Airway Facilities Environmental and Safety Compliance Program*. FAA Order 1050.17. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

2. *Utilization and Disposal of Excess and Surplus Personal Property*. FAA Order 4200.2. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

3. *Removing an Obsolete Solution.* FAA Acquisition Management System, Section 2.8. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC. http://fast.faa.gov/.

4. *Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities.* FAA Order 1050.10C. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.